Denmark

Breitenbauch, Henrik Ø.

Published in:
Comprehensive Security and Integrated Defence

Publication date:
2014

Document version
Publisher's PDF, also known as Version of record

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Report

Comprehensive Security and Integrated Defence:

Challenges of implementing whole-of-government and whole-of-society approaches

Tomas Jermalavičius, Piret Pernik, Martin Hurt

with
Henrik Breitenbauch
and
Pauli Järvenpää

ISSN 2228-0529
ISBN 978-9949-9448-3-5

International Centre for Defence Studies
Toom-Rüütli 12-6, 10130 Tallinn, Estonia
info@icds.ee, www.icds.ee
Tel.: +372 6949 340
Fax: +372 6949 342

Table of contents

Acronyms

3D – Defence, Diplomacy, Development
C4I – Command, Control, Communications, Computers and Information
CA – Comprehensive Approach
CBRN – Chemical, Biological, Radiological and Nuclear
CDM – Collaborative Decision-Making
CEDTE – Centres for Economic Development, Transport and the Environment
CEP – Civil Emergency Planning
CIP – Critical Infrastructure Protection
DEMA – Danish Emergencies Management Agency
EOD – Explosive Ordnance Disposal
EU – European Union
FSF – Danish Peace and Stabilisation Fund
ISAF – International Security Assistance Force
ISS – International Security Strategy
IT – Information Technology
MEAC – Ministry of Economic Affairs and Communications
MFA – Ministry of Foreign Affairs
MOI – Ministry of the Interior
MOD – Ministry of Defence
MSA – Ministry of Social Affairs
MSB – Swedish Civil Contingencies Agency
NATO – North Atlantic Treaty Organisation
NAVI – National Advisory Centre for the Critical Infrastructure
NCC – National Crisis Centre
NCTb – National Coordinator for Counter-Terrorism
NDDP – National Defence Development Plan
NDS – National Defence Strategy
NGO – Non-Governmental Organisation
NSC – National Security Concept
NSS – National Security Strategy
ODA – Official Development Assistance
OECD – Organisation for Economic Cooperation and Development
PET – Danish Security and Intelligence Service
RSAA – Regional State Administration Agencies
SOP – Standard Operating Procedure
SOVI – Strategic Council for the Critical Infrastructure Protection
TTP – Tactics, Techniques and Procedures
UAV – Unmanned Aerial Vehicle
WGA – Whole-of-Government Approach
WSA – Whole-of-Society Approach

Executive summary

S1. This report identifies conditions for the successful interactions of national security and defence stakeholders in the strategic framework of comprehensive security and integrated defence. It reviews the literature on comprehensive and integrated approaches to complex security and defence challenges and extracts some key factors underpinning the effective whole-of-government and whole-of-society efforts. It then considers experiences of several nations – Denmark, Finland, The Netherlands and Sweden – in building integrated security and defence systems. Finally, the paper investigates the 'state of play' in Estonia when it comes to implementing the concept of integrated defence. It closes with the recommendations to Estonia's policymakers.

Part I: Stakeholder Interactions in Comprehensive Security – Conditions for Success

S2. In this part, the paper argues that the nature of contemporary security and defence requires a concerted planning, preparation and action by governmental and non-governmental stakeholders, as no single organisation possesses a full spectrum of capabilities required to deal with complex, multidimensional and dynamic set of threats and risks. This applies equally to the activities at the stages of threat prevention, active countering of actual threats and the management of their consequences. The same logic also extends to civil emergencies or crises as well as to wars and operations other than war, both on home soil and abroad.

S3. Conditions and measures enabling and facilitating cooperation, coordination and collaboration between various stakeholders in order to achieve congruence and synergy of their effort are required at different levels. At the national level, the nation's governance and strategic cultures should be favourable to bringing different civil security agencies and the military together for common planning and operations, instead of purposefully keeping them apart. There must also be a broad consensus over the security and defence objectives and ways of meeting them.

S4. At the governmental level, structural and procedural reforms are required, such as establishing inter-agency 'issue-based' units; creating a proper cabinet level planning and oversight mechanism for the entire security and defence sector, supported with appropriate inter-agency planning methodologies, doctrines and training programmes; harmonising planning approaches of various ministries; and increasing capacities for flexible networking with non-governmental stakeholders in policymaking as well as in planning and conducting security and defence operations.

S5. Individual agencies should be cognisant of the roles, objectives, resources, capabilities and working practices of different stakeholders as well as appreciate the costs and benefits of interacting with them. Equally important is their readiness for such interactions, ranging from appropriate physical infrastructure to organisational procedures and structural arrangements which allow connecting with other governmental as well as non-governmental and private sector organisations. They should dedicate sufficient resources for common training with other stakeholders, while their leaders should be

promoting the internal atmosphere and culture encouraging collaboration with other organisations.

S6. The paper finds that conditions even at the team and individual levels are very important to successful interaction of security and defence stakeholders. Multi-organisational teams should have a shared understanding of the problems they are tasked to address as well as use unified terminology. Common training, shared physical space, trust-building and appropriate team leadership styles are also extremely important elements. However, eventually the entire edifice of executing the comprehensive approach rests on the cadre of security and defence professionals possessing a broad outlook on security, multi-agency working experience and appreciation of differences in the organisational and professional cultures of various stakeholders as well as the ability to build and maintain relationships with those stakeholders. Culture shifts, major organisational changes and behavioural models supporting the whole-of-government/whole-of-society approach cannot emerge without human resources nurtured and managed in the spirit of collaboration.

S7. Part One concludes that parliaments have an ever important role to play in shaping the above conditions at all levels. These range from encouraging frank and robust strategic debate on comprehensive security and defence as well as passing legislative measures designed to reduce organisational 'stovepipes' in the government, through exercising government's accountability for reforms in the security and defence sector, and to endorsing candidates for leading executive positions possessing the necessary credentials for the whole-of-government/whole-of-society approach.

Part II: National Approaches and Experiences

S8. Collaboration between different actors responsible for national security, in all of its aspects, has long and successful historical tradition in **Finland**. Until the 1990's, the focus was on how to best marshal the nation's resources to support military defence. Since then, emphasis has been increasingly laid on 'comprehensive security', where military defence is just one, albeit important, of the many aspects of security. The aim now is to secure the 'vital functions of society' in a common effort where the state and municipal authorities, the business community, and the various non-governmental organizations collaborate with each other to produce highest possible security for the Finnish citizen. On the national level, this effort is coordinated by a special committee, the Security Committee (previously known as the Security and Defence Committee), which has the task of monitoring, planning, preparing, coordinating and implementing all the measures taken to improve Finland's comprehensive security.

S9. Since the millennium, challenges and initiatives have been most prevalent in the external domain of **Denmark's** policy. This means the efforts have been focused in the development of particular and general Danish policies and processes with regard to civil-military interaction in stabilization missions as well as in contributions to wider peace-time stabilization of fragile states. Nonetheless, the internal dimension has also been subject to a set of challenges and initiatives. This is notably in emergency management policy where, for instance, the principle of sector responsibility (distributed governance) has been

under pressure by both cross-cutting challenges like cyber-security but also, in regulatory terms, by increased demands from the European Union. Apparently too small to establish formalized cross-cutting coordination and implementation but big enough to be stove-piped, the Danish central administration and its agencies have struggled to identify and implement effective processes and institutionalized approaches to comprehensive approach and whole-of-government mechanisms both at home and abroad. A set of mechanisms has nevertheless been established which has furthered Danish government's ability to monitor, implement and plan whole-of-government policies. As a result, Danish government abilities to address the new cross-cutting challenges have improved.

S9. **The Netherlands'** security policies place a strong emphasis on comprehensive solutions to external and internal security challenges. Coordinated deployment of instruments available to the government and relevant in particular circumstances, or 'integrated approach', is a well-established principle. Despite that, its policy framework remains, by and large, split into the external (International Security Strategy) and internal (National Security Strategy) vectors, even though they overlap to a certain degree. Both strategies stress the importance of mutual awareness between security stakeholders as well joint threat assessments, analysis, planning and learning mechanisms in implementing the integrated approach. Planning and conduct of the external missions is benefiting from a structured, systematic, comprehensive and evidence-based Collaborative Decision-Making (CDM) model, which includes such key stakeholders as defence, foreign affairs and security and justice ministries and which covers political, economic, social and security aspects of missions abroad. It is currently being elevated from the operational and tactical to a strategic and political level of decision-making. The country is also very systematic in defining and pursuing, through the NSS, main building blocks for the whole-of-government activities. This includes government-wide analysis (strategic foresight, thematic in-depth studies and scenarios, short-term horizon scanning and national risk assessment), strategic planning and follow-up.

S10. Until the end of the Cold War, **Sweden's** Total Defence system focused on maintaining readiness to defend the nation against an armed attack. The primary role of civil defence was to support the Armed Forces. When the military threat disappeared in the first half of the 1990's it took only a few years to dismantle the Total Defence system. Organisations were disbanded, planning and exercises were cancelled. The Swedish Armed Forces were reorganised and focused on operations outside Swedish territory. A new civil crisis management system is being introduced but progress has been relatively slow compared to the dismantling of the old Total Defence system. Due to radical changes in civil society, the new system has to tackle today's challenges in a different manner compared to the system that was in place during the Cold War.

S11. Part Two concludes that, in all four countries that the report has covered, comprehensive thinking in security affairs emerged gradually and is manifested in a variety of ways. A striking feature in all cases is the centrality of defence organisations to the efforts to implement comprehensive security concepts. This is partly due to their set of missions, which include both external and internal functions and which span the entire spectrum of situations – from peacetime

through crises to wars. This often makes them the central hinge on which comprehensive operations rely. It is also partly the legacy of total defence paradigm, where defence owned, operated or relied upon large systems (including voluntary defence organisations) necessary to channel society's resources to support military defence efforts. The challenge is how to build upon this legacy in creating and running whole-of-government/whole-of-society systems in pursuit of comprehensive security.

Part III: The 'State of Play' in Estonia – Challenges of Implementing Integrated Defence

S12. Based on the interviews with government officials it was identified that a key facilitator for the application of the whole-of-government approach is broad consensus on the underlying principles of the integrated national defence across all government actors. The need to implement integrated national defence has been widely accepted and supported across all actors of the government. It has been generally accepted that all actors have defined roles and responsibilities to ensure national defence.

S13. The everyday operational inter-agency interaction in crisis management and in the area of civilian support to the military is good, even though the need for greater formalization and regulation of interactions as well as for more practical inter-agency training and exercises was noted.

S14. Major obstacles to the implementation of the integrated defence are rigid and outdated mindsets and divergent philosophical understandings across the ministries and their agencies concerning the essence of the integrated national defence; lack of strategic and long-term planning traditions, procedures, regulations and instructions across all governance domains and policy subjects; lack of competence, know-how, human and financial resources that inhibit strategic planning efforts; and insufficient attention to managing inter-agency collaboration.

S15. Deficiencies with potentially negative implications for national security are lack of whole-of-government preparations for wartime responsibilities and duties (no legal mandate, attribution of financial resources, and no strategic and operational planning in some policy areas); lack of clarity regarding the leadership and command structure during some escalation stages (emergency situation, state of emergency, wartime), and lack of mandate for a coordinating ministry to apply coercive measures if other government actors do not fulfil their duties.

Conclusions

S16. The report concludes that committing to a course towards whole-of-government and whole-of-society approaches is obviously an ambitious undertaking with very broad implications as to how security and defence affairs should be conducted. Given the scope of the challenge, it is not surprising that many countries are making a rather slow progress towards effective whole-of-government and whole-of-society approaches to security and defence. In many regards, Estonia does not stand out as a laggard in pursuing its own whole-of-government and whole-of-society solutions. The conceptual basis is in place,

even if in need of some fine-tuning. Many legal, institutional and organisational elements are also emerging, reinforced by various positive examples of operational collaboration as well as involvement of non-governmental and private sectors. However, there are many weaknesses too, concentrated in the areas of strategic planning culture and organisational competence; availability and management of human resources; knowledge management (especially in translating implicit knowledge to explicit through manuals, handbooks and guidelines); management of inter-agency processes in security and defence as well as management of stakeholder expectations. Resolving them will take time, sustained effort, much good will and patient leadership.

Introduction

This report was produced in response to the knowledge requirement formulated by the Defence Commission of the Estonian Parliament (Riigikogu), in order to stimulate thinking and debate about the implementation of comprehensive security and integrated defence concepts.

Estonia's capstone national security and defence documents – National Security Concept and National Defence Strategy – established integrated defence and comprehensive security as fundamental principles upon which to base the nation's response to a complex and dynamic global, regional and national environment of security challenges, risks and threats. However, to have a real impact, these principles have to be translated into the requisite institutional arrangements, practices and culture, enabling genuine and sustainable integrated – whole of government and whole of society – approach.

The research undertaken in response to the requirement by the ICDS aimed to generate a set of recommendations on the implementation of comprehensive security and integrated defence principles in Estonia. More specifically, it sought to:

- Identify a set of conditions for the successful implementation of a whole-of-government/whole-of-society approach to security and defence;
- Investigate selected foreign practices in implementing whole-of-government/whole-of-society approach to security and defence;
- Recommend changes and improvements in the institutional arrangements and practices in Estonia.

The project was based on qualitative research methodology. It included desk research focusing on literature which generalises the post-Cold War concepts and experience of NATO and the EU countries in pursuing comprehensive solutions (e.g. in crisis response operations, complex emergencies management, homeland security and defence activities). From this, the generic enablers of successful whole of government/whole of society approach at different levels were derived. The project also included 'side-sight' research, or case studies – desk and field research into the concepts, arrangements and practices existing in several small NATO and the EU countries. This yielded further insights into the challenges and 'best practices' of implementing whole of government/whole of society approach to security and defence. Finally, drawing upon desk research and an extensive series of interviews, 'state of play' in Estonia was ascertained, in order to identify various positive developments as well as weakness in the country's efforts to implement comprehensive security and broad-based defence concept.s

In Part I, the report identifies the conditions for the successful interactions of national security and defence stakeholders in the strategic framework of comprehensive security and integrated defence. It reviews the literature on comprehensive approaches to complex security and defence challenges and extracts some key factors underpinning the effective whole-of-government and whole-of-society efforts. In Part II, it then considers experiences of several nations – Denmark, Finland, The Netherlands and Sweden – in building integrated security and defence systems. Finally, in Part III, the paper

investigates the 'state of play' in Estonia when it comes to implementing the concept of integrated defence. It closes with the recommendations to Estonia's policymakers.

Part I: Stakeholder Interactions in Comprehensive Security – Conditions for Success[1]

Introduction

The philosophy of comprehensive security is put into practice through the interactions of various security and defence stakeholders: government agencies, public sector and non-government organisations, private sector enterprises and local communities. 'Collaboration', defined as 'the action of working with someone to produce something' (Oxford Dictionary), is thus a critical concept in implementing a broad approach to security and defence, although this is not the only possible form of interaction.

The aim of this part of the report is to identify a set of conditions at various levels (national, organisational, team and even individual) which enable and facilitate interactions, especially collaborative ones, between security and defence stakeholders. It draws upon the literature concerning the Comprehensive Approach (CA) – the term referring to the concerted action of military and non-military actors in a theatre of operations – as well as on related concepts such as 'interagency cooperation' and the 'whole-of-government' approach.

Although the term 'Comprehensive Approach' has been devised with a particular kind of operation in mind ('out-of-area' crisis response, stabilisation, peace support and counterinsurgency), many of its tenets are also applicable in the domestic setting. In this setting, civilian actors have to support the military, and vice versa, in a wide range of circumstances – from civil emergencies through security crises to military contingencies, including defence against military aggression.

Both 'out-of-area' and domestic civil and military operations are 'complex operations' – involving multiple actors; combining many dimensions (political, military, technological, informational, human, environmental, economic, etc.); and dealing with a great number of dynamic factors and many uncertainties. It is therefore assumed that the conditions for collaboration sought by the proponents of a CA are also relevant, to a large extent, in ensuring collaboration amongst stakeholders in national broad-based defence and comprehensive security.

I.1. Setting the scene: some terminology issues

Over time, policy and academic discourses have adopted a number of terms to depict a holistic approach to security and defence, and the principle of a broad and multifaceted response to complex security challenges. Those of greatest relevance to this enquiry, in the descending order of their breadth, are:

[1] By **Tomas Jermalavičius**, Research Fellow, ICDS (tomas.jermalavicius@icds.ee)

- **Comprehensive security**, which is 'the end-state of a nation's security policy achieved through the coordinated application of the multiplicity of government and non-government components and instruments involved in developing and maintaining a stable and peaceful environment that permits the effective operation of political, economic and social institutions for the overall benefit of citizens' (Fitz-Gerald & Macnamara, 2012: 4).
- **Comprehensive Approach** (CA), understood as the 'interaction between various actors and organisations with the aim of generating coherent policy and action during periods of crises or disaster or in a post-conflict environment' (Hull, 2011: 5).
- **Whole-of-Society Approach** (WSA) to complex threats and risks, which refers to 'multi-sector, inclusive approaches that unify the experiences and resources of government, military, civil society, and the private sector' (Prevent Project, 2011: 27).
- **Whole-of-Government Approach** (WGA), which at the most fundamental level is a public administration model where 'horizontal co-ordination and integration are embedded in the process of policy design and implementation' (OECD, 2011: 14), or which takes the form of 'concerted and coordinated interagency effort to apply all elements of government power' (Stickler, 2010: 4).[2]

It is also necessary to note that the interactions between various actors and organisations in security and defence can take many forms and levels. According to Stickler (2010: 7), these range from very **basic (consultation)** and **elementary (cooperation)** to **intermediate (coordination)** and **advanced (collaboration)** (the features of each are briefly described in the table below).

Interagency Maturity Levels	**Basic Elements Contributing to Overall IA Maturity Level**				
	Interagency Relationships	**Information Access**	**Agency Goals**	**Agency Attitude**	**Interagency Process**
Basic (Consultation)	Minimal	Restricted: Briefings confined to specific actions underway	Independent; frequently conflict	Self-absorbed	Sporadic
Elementary (Cooperation)	Personal	Limited: Information exchanged to deconflict operations, to stay out of each other's way	Independent but aware of others	Friends could be helpful	Unstructured
Intermediate (Coordination)	Organizational	Expanded: Willing to share future plans to garner mutual support	Independent but aligned with others	Friends are essential	Organized
Advanced (Collaboration)	Institutional	Extensive: Information flow supports full planning cycle and integrated operations	Mutual and reinforcing	Cannot do it alone	Systematic

Table: Interagency maturity levels (Stickler, 2010: 7)

[2] More definitions of various terms used in security and defence discourses, including in Estonia, are provided in the Appendix.

I.2. Conditions at the national level

One of the first factors determining the ease with which a particular nation's civilian and military agencies, as well as other organisations, interact is the **tradition and culture of its security governance**. In many nations concerned about the inherent power of the military and the possibility of its misuse, and in nations with a strong tradition of 'checks and balances', there is a strict legal separation of the armed forces and other security organisations (Miani, 2010). The importance of this separation is built into the very constitutional fabric of the nation. It is also often manifested in strict limits placed on the peacetime activities of the military on domestic soil, to the point of banning the military from directing any civilian activity.

In the context of such a tradition and culture, military and civilian organisations lack the habits, incentives and arrangements that would facilitate their collaboration; they tend to stick to their 'stovepipes', defend their turf and hold rather hostile views of one another. Even after 9/11 – with the ensuing emphasis on better integrated homeland security solutions and on a comprehensive approach in overseas operations –change in such nations is taking place very slowly. For instance, only recently, following a ruling of its Constitutional Court, Germany has begun to allow a very limited role for its armed forces on German territory to counter assaults which threaten 'catastrophic consequences' (BBC News, 2012). The US, meanwhile, is struggling to integrate diplomacy, development and defence instruments in theatres of operations, often without a corresponding alignment of the respective agencies in the capital (Schnaubelt, 2009).

At the other end of the spectrum, there are countries with a long-standing tradition of 'total' defence, adept at thinking about and preparing to deploy all national resources to meet the overriding objective of fending off military aggression, or countries with experience in fighting protracted insurgencies, where the boundaries of military and civilian (law enforcement, intelligence, security) organisations have blurred and their activities intermingled. This experience is particularly applicable today, when the dividing lines between external and internal security are becoming obscured due to the rise of trans-national security issues such as terrorism, proliferation of weapons of mass destruction, organised crime, disruption of critical infrastructure and services (e.g. by means of cyber attacks), etc. (Lutterbeck, 2005).

In practice, these conditions may not necessarily lead to a smooth WGA: indeed, competition between various agencies could be just as pronounced or, in the case of a total defence mind-set, one agency (the military) might be too dominant. On the other hand, such a tradition and culture within security governance leads to more experience with cooperation, coordination and collaboration, better informal networking habits and more positive attitudes towards the criss-crossing of agency lines and the reaching out to all relevant stakeholders (e.g. as in the UK; see Baumann, 2010). Involving non-governmental stakeholders in overall security and defence efforts also comes more naturally to such security governance cultures.

A second powerful national-level factor determining the intensity of interaction between various agencies is the existence of meaningful (as opposed

to superficial) **political, strategic and societal consensus** regarding the overall national security ends, ways and means, and regarding the goals of participating in particular civil-military operations (Stepputat, 2009; Fitz-Gerald & Macnamara, 2012). Without such a consensus, different actors within and outside government find it difficult to relate their mission, daily activities and initiatives to a broader picture and with one another; they become driven by narrow agency interests and short-term opportunities (Jennings, 2010).

In turn, reaching a meaningful political and strategic consensus requires a **culture of continuous dialogue and compromise**, which is itself hard to achieve in the highly competitive realm of politics and amidst rivalry for limited resources. As Rotman (2010: 4) puts it when writing about national-level fragmentation as an obstacle to CA, 'all major players needed for a truly Comprehensive Approach face bureaucratic and political incentives that largely favour parochial interests over investing in common solutions'.

I.3. Government level conditions

To overcome the institutional fragmentation and to make WGA work, it is often necessary to undertake certain **government-level procedural adjustments and institutional restructuring**.

First and foremost, this entails creating and maintaining a proper **joint cabinet-level analysis, planning, coordination, monitoring, evaluation and funding mechanism** through which multifunctional strategies can be processed. In most cases, this requires a cabinet-level unit dedicated to coordinating security and defence policies and strategies as well as amalgamating the inputs (including financial ones) of various agencies. In addition, **'issue-based units'** (e.g. counter-terrorism, cyber security, etc.) under cabinet supervision and staffed by personnel from various agencies, are necessary to overcome institutional 'stovepipes' and address the issues which cut across agency lines (Stepputat, 2009; Miani, 2010; Hull, 2011). As Fitz-Gerald and Macnamara (2012: 6) argue, 'the efforts of one unit within a ministerial portfolio on its own neither will, nor should, provide the leadership and *modus operandi* for comprehensive security'.

Furthermore, civilian agencies in particular need to grapple with the fact that, compared to military organisations, they lack **vertical integration** as 'they do not have the equivalent of operational level headquarters to bridge the gap between national-level policy/strategy and tactical actions on the ground' (Schnaubelt, 2009: 37). This makes civil-military integration at the operational level particularly difficult and often leaves no choice but to rely, for operational planning purposes, on military command structures with a few civilians inserted into them – hardly an optimal organisational solution for 'complex operations' in which the military's contribution is just a small part of the overall effort.

On the other hand, it has often been noted that broad and ambitious organisational reforms undertaken by governments in order to enable WGA and CA have not taken off in most countries, while more limited process-oriented changes (especially in joint planning and inter-agency project management) have been more useful. These lesser measures 'have helped to reduce transaction costs, facilitate communication among departments, and pool expertise and

resources from different corners of the government architecture' (Baumann, 2012: 36), but without threatening the organisational identity of separate agencies.

Coherence of government policy and an overarching consensus-based vision for security and defence matter a great deal in facilitating interaction between different agencies and non-governmental stakeholders. As Jennings (2011: 105) puts it, 'in the absence of an integrated strategic vision, agencies go rogue – driven by mandates, not strategy'. According to Hull (2011: 8), it assumed that 'a government's engagement in a conflict or disaster will cost fewer resources and be more likely to achieve greater and more sustainable impact if the ministries share the same understanding of the problem and have a shared and well-sequenced strategy to address it'. However, this has to be supplemented with efforts to harmonise the strategic planning, capability development and operational deployment processes and practices of the various governmental organisations with a role in national security and defence.

Different organisations employ different planning methodologies, are driven by varying time horizons and have very different approaches to building capabilities, managing projects and exercising leadership, making their cooperation, coordination and especially their collaboration quite complicated tasks. These differences are especially pronounced between civilian agencies on the one hand and military organisations on the other, but they also exist between various civilian agencies. As Schnaubelt (2009: 41) notes:

> The military in some ways is like a fire department – only a relatively small portion of its total number is engaged in operations at any particular time. The remainder is in reserve waiting for a call to action, or in training, or undergoing a 're-set' to prepare for a specific future operation. Civilian agencies are more like a police department – nearly all of their personnel are engaged in current operations with almost no float for training and virtually none being held in reserve.

Governments are thus advised to 'establish **a permanent, enduring, and robust education, training, doctrine, materiel and organisational approach** among the various agencies' (Caslen & Loudon, 2011) involved in 'complex operations' which require cross-functional inputs and inter-agency efforts.

Interaction between government agencies is also often hampered by a lack of **technical and administrative interoperability**, especially when it comes to Command, Control, Communications, Computers and Information (C4I), logistics, various standard operating procedures (SOPs), knowledge management systems (data collection, fusion and sharing) and even personnel management (e.g. rotation cycles). Indeed, interagency interoperability – or 'thick and frequent interaction among the organisations and individuals involved in complex engagement spaces as they engage in planning, decisionmaking and operations' (Hallett & Thorngren, 2011: 42) – should be considered as part of an agency's capability set (other capability components being Doctrine, Organisation, Training, Materiel, Leadership, Personnel and Facilities).

Extending this aspect further, it should be noted that, at the strategic and operational levels, all governmental agencies must have **a common operating picture**, built by fusing data from different sources and agencies and through this develop a common understanding of complex security situations (Bryan & Pendall, 2010: 5). As Strickler writes (2010: 6), 'information exchange or

information sharing is a fundamental building block of cooperative efforts'. This is hardly possible without technical and procedural interoperability.

If the WGA is often impaired by legal, cultural, organisational and technical issues, it is even more difficult to achieve a WSA. CA proponents argue for the integration, or at least consultation, of non-governmental partners in the joint effort of drafting strategies, policies and their implementation plans, and in the planning and conduct of operations. However, the diversity of such partners – ranging from humanitarian and development NGOs to private contractors, each with very diverse missions, objectives, cultures, identities, principles, practices, resources and capabilities – makes this a particularly challenging undertaking. For instance, for humanitarian organisations, 'independence, impartiality and neutrality is the common denominator' (Friis, 2010: 19); they distance themselves from politically-motivated activities, and differ significantly in their views on the use of force or in decision-making styles from, for example, military organisations (Egnell, 2013).

Thus, one of the key preconditions for involving non-government actors in security and defence efforts is an ability to practise **flexible, networked forms of interaction** with them (Baumann, 2012; Lira, 2010), rather than trying to prod them into a hierarchical relationship and command them with top-down directives. It also requires a capacity to be selective in the kind of interaction that is pursued with these actors (e.g. only consultation and de-confliction of activities in the theatre of operations, or coordination and close collaboration). Government inter-agency operational and strategic headquarters need to ensure that the necessary infrastructure (e.g. non-classified communication networks and databases) is available to 'plug' trusted and relevant non-governmental actors into governmental processes, so as to be able to seamlessly exchange information, consult, coordinate and collaborate with these actors.

I.4. Agency, team and individual level considerations

Many prerequisites for a successful WGA lie within the agencies themselves and may require efforts to make internal reforms and adjustments. The type and nature of a particular mission, however, will strongly determine how those agencies define themselves and conduct their business. As Jennings (2011: 91) explains, 'differences stem from competing institutional mandates, missions, legal and resources constraints, as well as culture, mind-set, strategic outlook and expectant time horizons.'

Miani (2010; 13-14) distinguishes between **process-oriented organisations** (such as a diplomatic service for which operations 'can never truly end' and there are in any case no perfect solutions, only sub-optimal outcomes; thus they see little need to engage in thorough planning) and **goal-oriented organisations** (such as the military, whose 'operations are divided into discrete events that have identifiable start and end points' and where optimal outcomes can be defined, along with detailed plans to achieve them). In a similar vein, cultural differences flowing from the nature of mission exist between the civilian agencies (intelligence, law enforcement, rescue, etc.).

I.4.1 Agency characteristics

Cultural differences are more difficult to address within agencies than structural or legal obstacles. Agencies which succeed in the WGA and WSA setting, despite the above differences identified by Miani, are usually distinguished by the following key characteristics:

(1) **Ability to identify other actors of importance** to their mission or to particular tasks (Petersen & Binnendijk, 2007; Hull, 2011);

(2) **Good understanding of those actors**: their missions, responsibilities, cultures, motives, goals, working practices, resources, capabilities, comparative advantages, weaknesses and strengths, as well as their added value in resolving various security issues. Conversely, they also are cognisant of which of their own capabilities and resources are relevant to the missions and tasks of other actors, as well as the circumstances in and the means by which they can be provided (Davidson et al, 1996; Schnaubelt. 2009; Bryan & Pendall, 2010; Lira, 2010; Hallet & Thorngren, 2011; Hull, 2011; Fox, 2011; van der Goor & Major, 2012).

(3) **Understanding of the tangible benefits** of cooperation, coordination and collaboration with those actors (i.e. they recognise existing interdependencies), as well as the **costs and limits** of those interactions. The latter are particular pertinent as regards the involvement of various non-governmental actors, some of whom do not wish to be seen as adjuncts to the government (Caslen & Loudon, 2011; van de Goor & Major 2012; Baumann, 2012).

(4) Having the **internal arrangements** necessary to interact with external actors (e.g. clear points of contact; binding exchange procedures; flexible command and control, enabling quick plug-in by other organisations; shared 'lessons learned' databases, etc.) (Davidson et al, 1996; Petersen & Binnendijk, 2007; Lindley-French, 2010; Hull, 2011).

(5) Dedicating **sufficient resources** for WGA and WSA-related interactions, and **especially for training** together with other agencies (Strickler, 2010; Fox, 2011).

(6) Promotion and support by **senior leadership** of 'atmospheres where the spirit of cooperation, collaboration and teamwork is encouraged, and where the negative effects of suspicion, infighting, and self-interested agendas are eliminated' (Caslen & Loudon, 2011: 9).

These characteristics allow agencies to act as **'smart customers'** of services provided by other agencies, and to be 'smart providers' of their own services to other agencies.

I.4.2 Team characteristics

Once inter-agency 'working groups', 'task forces' or 'issue-based units' have been formed to advance a comprehensive security agenda, the success of a WGA to a large extent rests on the dynamics within these teams. The main factors facilitating their work – be it at the strategic, operational or tactical level – include:

(1) **Shared assumptions and understanding** of the task or problem at hand, the team objectives, the mix of available tools and competences, and the impact of the team's outcomes on the overall strategy (Lacquement, 2010; Jennings, 2011; Lindley-French, 2010; Lira, 2010);

(2) **Unified language (terminology), formats and style of communication** (Waddell, 2011; van der Goor & Major, 2012; Davidson et al, 1996). As Caslen and Louson (2011: 12) articulate, 'introducing a common language for interagency efforts would help eliminate the confusion associated with the various terminologies unique to each agency';

(3) Ability of a team to **harness the unavoidable frictions** between its members from diverse backgrounds: 'While often perceived as an indicator of failure, confrontation and friction among organisations may well be signs that a genuinely comprehensive approach is at work' (Baumann, 2012: 42);

(4) **Nuanced peer-leadership style** (Bryan & Pendall: 2010) rather than the hierarchical, top-down, commander-centric approach inherent to military organisations. As Schnaubelt (2009: 66) observes, 'civilian leaders will typically expect to be treated as equals rather than subordinate to the military commander.' This is especially important in teams whose participants include non-governmental stakeholders, who do not appreciate a 'command and control' approach and need to be persuaded rather than ordered to contribute or coordinate;

(5) For operational and tactical inter-agency teams, **common team training** is essential (Fox, 2011), to the point that it is desirable that operational teams are drawn from the same people who trained together (a natural order of things for mobilised military reservists, but somehow not for civil-military teams). For strategic-level inter-agency teams, a **common educational background** (e.g. from inter-agency courses and programmes) and **mutual awareness** training is very important;

(6) **Shared physical space** (Hull, 2011; Hallett & Thorngren, 2011). The rise of technological means enabling virtual collaboration over distances is very beneficial in terms of cultivating 'communities of practice' to share knowledge across organisational boundaries. However, teams working within a shared physical space perform better in terms of congruence of effort, communication and coordination effectiveness, etc. Thus, as Hallett and Thorngren (2011: 45) put it, 'the main question in facilities related CA capability development is "Do our facilities make interaction easier, or create additional barriers to interaction?"'.

I.4.3 Individual characteristics

Success in the CA setting is also shaped by factors even at the individual level. This is a reality worth taking into account by organisations (such as parliamentary committees) which have a role in selecting, vetting and appointing individuals for key positions crucial to implementing comprehensive security and defence strategies and cross-cutting policies. CA requires a cadre of highly knowledgeable, goal-oriented and diplomatic individuals in the right places and at the right time. Such individuals should possess and continuously demonstrate:

(1) A **'generalist' profile** and an **ability to move and work between different agencies**. In some countries, there has been a talk of creating a pool of 'national security professionals' (Baumann, 2012) with a 'comprehensive' mind-set and skills (i.e. possessing a holistic view of the national security system and positive attitudes towards collaboration) (Bryan & Pendall, 2010);

(2) **Ability to appreciate and handle differences in the professional cultures** represented in the inter-agency teams (Rotmann, 2010);

(3) **Agility, adaptivity and ability to see trends and opportunities** emerging in a complex strategic, operational and tactical environment (Caslen & Loudon, 2010);

(4) Highly developed **inter-personal skills and ability to connect and build relations** with other stakeholders. As Caslen and Loudon (2011:11) put it, 'partnerships are defined by value of mutual benefit, developed by interpersonal skills'.

(5) **Negotiation, persuasion and indirect influence skills**, which arenecessary to build consensus and shape the outcomes of multi-stakeholder interactions in a way that does not antagonise the various actors important to a particular mission or to the overall security and defence strategy (Lacquement, 2010).

As such individuals do not appear overnight, governments have to invest significant resources, time and sustained effort to build **professional education, development, advancement and evaluation programmes and personnel rotation systems** which promote and reward the above traits. As Lacquement (2010: 10) writes, 'a key approach is to do more to educate the leaders of both communities [civilian and military – T.J.] to be better prepared for <…> complex security challenges. Among the means that can help accomplish this are education, training, development, and assignment policies that do more to share the relevant expertise of civilian and military leaders across their respective domains' and '…to ensure that the ranks of civilian and military leaders include generalists who can make such complex operations work'.

Culture shifts, fundamental organisational changes and behavioural models supporting WGA and WSA cannot emerge without human resources nurtured and managed in the spirit of collaboration. This is perhaps the most important lesson which governments pursuing comprehensive, integrated solutions to contemporary security challenges have often failed to heed.

Part I Conclusions

Acknowledging the multi-dimensional and dynamic nature of contemporary security and defence entails accepting that effective solutions to national security challenges cannot come from separate organisations, or even nations. This applies equally to activities at the stages of threat prevention, active counter-activities and the management of consequences. The same logic also extends to complex emergencies or crises, to wars, and to operations on home soil and abroad. The national agencies responsible for managing the various aspects of security have to reach out beyond their organisational and national boundaries in order to succeed. Concerted efforts by governmental,

non-governmental (including the private sector and the academia), inter-governmental and supra-national actors are often the key to resolving national, regional and global security issues.

Even when the management of a security situation falls within the area of responsibility of a particular single organisation, its resources might not be sufficient to cope with adverse circumstances. This would necessitate the marshalling of the resources of other organisations – be they governmental, public or private, foreign (allied) or national. Thus WGA, WSA and, furthermore, whole-of-alliance imperatives are particularly strong in small states, both in the case of large-scale emergencies or crises and in wartime.

In turn, the success of a comprehensive and integrated response to complex national security challenges rests on the ability of the involved actors to cooperate, coordinate and collaborate. The particular choice of the form of interaction is context-specific: it depends on the particular contingency, its demands, and the character of the organisations which are responsible for managing it or can add value to this effort. It is clear, though, that many general conditions must be in place in order for those interactions to succeed. These conditions span the national, governmental, single organisation and even team and individual levels.

Key Insights from Part I

- Parliaments have an important role in shaping the conditions for success at all levels.
- They can **shape the nation's political and strategic debate** and, eventually, culture so that it moves in the direction of endorsing a comprehensive approach.
- They have **a special responsibility for forging a broad strategic consensus** in the country concerning the ways that the means and ends of security and defence are matched, with a particular emphasis on cooperation, coordination and collaboration in the framework of WGA/WSA.
- They can **stimulate adjustments in governmental architecture and practices** (e.g. long-term planning and budgeting, interagency concept development, interagency training) through cabinet accountability mechanisms (including budgetary appropriations).
- They can also work to **remove legal obstacles** hindering interaction between government agencies and create incentives for them to reform themselves in order to accommodate the demands stemming from WGA/WSA.
- They can even shape conditions at the individual level by **endorsing candidates** with the right credentials for a comprehensive approach for key positions in security and defence sector.

Part II: National Approaches and Experiences

Introduction

As part of this report, ICDS has looked at the experiences of several nations in building their WGA/WSA systems in the context of comprehensive security and the comprehensive approach in international operations. The four nations that have been chosen are either members of the EU or NATO (or both) and are relatively small. All four – Denmark, Finland, the Netherlands and Sweden – have been undertaking transformation of their security and defence systems since the end of the Cold War and, by and large, have been active in foreign missions and in addressing new cross-cutting security challenges. This part of the report describes the approaches, challenges and solutions found in these four countries.

II.1 Denmark[3]

II.1.1 Background

Since the turn of the millennium, cross-cutting challenges and initiatives have been most prevalent in the external domain of Danish policy, for example in the development of particular and general Danish policies and processes with regard to civil-military cooperation in stabilisation missions, as well as in contributions to the wider peace-time stabilisation of fragile states. Nonetheless, the internal dimension has also seen a set of similar challenges and initiatives, notably in emergency management policy where, for example, the principle of sector responsibility (distributed governance) has been under pressure from both cross-cutting challenges like cyber-security and, in regulatory terms, from increased demands from the EU.

In Denmark, the range of new security-related cross-sector tasks in the post-Cold War period has posed a fundamental challenge to the classical division of labour among ministries and agencies. Apparently too small to establish formal cross-cutting coordination and implementation, but big enough to be stove-piped, the Danish central administration and its agencies have struggled to identify and implement effective processes and institutionalised approaches to the comprehensive approach and to whole-of-government mechanisms both at home and abroad.

A set of mechanisms has nevertheless been established, furthering the ability of the Danish government to monitor, implement and plan whole-of-government policies. As a result, Danish government efforts to address the new cross-cutting challenges have improved over the period in question. Nonetheless, the impression remains that these changes have been relatively minor or even cosmetic in some cases. This points to a need for continued attention to the strengths and weaknesses related not only to the formal institutionalised approaches, but also to the role that the bureaucratic cultural

[3] By **Dr Henrik Breitenbauch**, Senior Researcher, Centre for Military Studies, University of Copenhagen.

preference for flexibility and informality plays with regard to inter-ministerial coordination and collaboration in Denmark.

II.1.2 External challenges and initiatives

In policies related to external security , including foreign, security, defence, development, and intelligence, Denmark has since the turn of the millennium been faced with a set of challenges which closely resembles those of other countries that have participated in international military interventions. Danish foreign and security policy has, since the end of the Cold War, been predicated on the increased geopolitical action space that resulted from the disappearance of the Soviet Union and the subsequent reduction in the role of Russia in Danish security geography. In an American world order, however, international institutions could not be taken for granted. Denmark coupled this concern with an ability to act more freely under the new setup to support international stability and the global institutions of the American order; Danish foreign policy has since been defined by the resulting so-called **activism**. While there is no formal capstone document capturing this position, it is nevertheless explained in a number of strategic guidance documents such as government plans, defence commission reports and strategic documents from the Ministry of Foreign Affairs (MFA) and Ministry of Defence (MOD) (e.g. Regeringen, 2011; Statsministeriet, 2013; Ministry of Defence, 2009, see also Breitenbauch, 2008).

In addition, an annual official statement on the state of Danish foreign policy is given by the Permanent Secretary of State for Foreign Affairs in the *Danish Foreign Policy Yearbook* (e.g. Grube, 2013). In practice, however, the overarching mechanism for steering Danish foreign policy is an informal consensus among leading politicians and civil servants about the general concept of activism, if not about its concrete application. This ambiguity allows for relative continuity in terms of level of ambition, even if every new government has applied new interpretations of degree, as can be seen in the changing government statement of plans (Statsministeriet, 2013).

Already in the 1990s, participation in international peace support operations in the Balkans made the Danish military an important element in Danish contributions to international order. The changed role of the Danish Armed Forces led to a greater emphasis on international missions in the 1999 **Defence Agreement** for 2000-2004 (MOD, 2013a). Danish defence policy is traditionally characterised by **broad Parliamentary support**, and participation in the development of the defence agreement, which normally runs for a five-year period, is seen a as a badge of maturity for political parties. The agreement covers budget, strategic rationales (tasks) as well as strategic and concrete planning and reforms, including all dimensions of defence policy such as personnel, materiel acquisitions, basing structure, etc. The document normally runs between 20 and 35 pages. Spokesmen for the political parties that have signed the agreement *de facto* act as part of a larger ministerial function -- as a kind of board for Danish defence policy.

Since 9/11, the interventions in Iraq, Afghanistan, Libya and Mali have demonstrated how central military missions have become to Danish foreign policy. In a trademark contribution to the ISAF mission in Afghanistan, Denmark provided a battlegroup (~750 men) from 2006-2014 in Helmand province and

Regional Command (South)/ Regional Command (South West), alongside the United Kingdom, Estonia and later the United States. The forces were deployed without national caveats and have been engaged in some of the most severe fighting in ISAF. Denmark has sustained one of the highest per capita casualty rates in ISAF. Before this major contribution to ISAF, Denmark notably contributed forces, again alongside the United Kingdom, in the Basra region following the invasion of Iraq in 2003.

Following a strategic review in 2003, **international operations became the primary raison d'être for the armed forces**, as set out in the 2004 Defence Agreement, which covered the period 2005-2009 (Bruun-udvalget, 2003; MOD, 2004a). Some domestic functions remained in terms of upholding sovereignty (air policing), search and rescue, VIP flights, environmental surveillance, as assistance in crisis management, etc. All these functions are described in the annual reports on Danish Defence (e.g. Defence Command Denmark, 2012). In conjunction with the 2004 Agreement, experience from the Balkan missions of the 1990s led to the announcement of a new major formal component of Danish security and foreign policy. Beyond the Agreement itself, a letter signed by the ministers of foreign affairs and defence announced a new framework for civil-military cooperation in these international missions (MOD, 2004). In the letter, the Danish word for comprehensive approach is **'civil-militær samtænkning'** or literally **'civil-military coordinated thinking'**. While the letter signalled a new ambition for cooperation in this area it also described the continuity of a clear demarcation of authority between the ministries. The 2004 Agreement also instituted **an inter-ministerial coordination body** with representatives from relevant ministries. As a consequence of the new Danish policy, Denmark also promoted the idea inside NATO as 'Comprehensive Planning and Action', which was later to become the 'Comprehensive Approach' (Fischer & Top Christensen, 2005).

'Samtænkning', however, as it was to become in daily parlance, has had **an ambiguous use and meaning** in Danish foreign and security policy ever since. The concept, in losing the 'civil-military' part has also doubled as a Danish version of 'whole-of-government' in general terms. In consequence, some confusion and suspicion has been attributed to the concept by various actors inside and, particularly in the case of the NGO's (which play an especially important role in Danish development policy), outside the government hierarchy.

Second, 'samtænkning', by virtue of its reference to the civilian and coordinating side of an equation sometimes dominated by military concerns, also became the glue which tied together the increasingly elaborate strategic *political* frameworks for Danish contributions, especially in Afghanistan (MFA and MOD, 2008; MFA and MOD, 2013). The history and functions of the concept are therefore more than operational and practical, and often *political* in the deep sense that its very ambiguity has been an important element in creating and sustaining broad political agreement to Danish foreign policy in these areas. A substantial role for 'samtænkning' in strategic guidance documents became a route for the left in Parliament (and the opposition) to agree to Danish policy.

In practical terms, the Danish WGA to international civil-military stabilisation missions has been developed on a case by case basis. The model developed from a very limited degree of cooperation between the embassy in

Bagdad and the Danish military contingent in Basra in the early phases of the occupation of Iraq. The lack of direct connection and support prompted the comprehensive approach letter in 2004.

Toward the end of the Danish efforts in Iraq, public debate about the lack of continuous monitoring and prioritisation (based on access to end-of-tour reports) led to pressure to increase the level of attention paid in Copenhagen. For the subsequent Afghanistan mission, this meant that from 2008 onward the political parties to the agreements in Parliament together with the government ministers and in coordination with international partners in Regional Command South, developed a set of strategic steering documents covering both Danish civilian and military contributions, . In spite of the steep learning curve in Iraq and later in Helmand, there was little formal change to the CA setup in Copenhagen, even if an Afghanistan task force was set up inside the MFA.

In 2009, concurrently with a critical evaluation of Danish CA efforts in Afghanistan (Stepputat, 2009; Schmidt, 2009) a **stabilization secretariat** was established inside the MFA. This small (and perpetually understaffed) unit is manned by the MFA (in principle 3-4 people) and the MOD (in principle 1-2, but in reality less). From the outset, the secretariat has been tasked with developing policy on fragile states and stabilisation, managing the daily running of the Peace and Stabilisation Fund, following operations, strengthening civil capacities for stabilisation, and gathering and processing lessons learned from this rather broad area.

Following international best practice, the **Danish Peace and Stabilisation Fund (FSF)** was founded in 2010 to fund efforts that fall partially outside military operations and Official Development Assistance (ODA) according to the OECD DAC criteria. To date it has funded three geographically motivated frameworks in Afghanistan-Pakistan, in the Horn of Africa and Maghreb-Sahel.

In 2010, a new coordination body manned by heads of department from the MOD, Defence Command, the Prime Minister's Office and the Ministry of Justice was formed to provide the leadership function for the stabilisation secretariat. This new **'comprehensive approach steering group'** meets about once every month and is formally tasked with being **the Danish forum for strategic and operational decisions regarding politically established frameworks for civil-military and stabilisation missions**. The steering group also has the authority to oversee the management of the FSF. In 2010, moreover, the MFA published a Danish policy toward fragile states emphasising the 'integration of activities ensuring a clear cohesion between Danish Foreign and security policy in relation to fragile states' (MOD, 2010, ii).

Denmark's armed forces do not formally make independent doctrine as the country relies on NATO doctrine, but do make use of TTP (tactics, techniques and procedures) that are not publicly available. There are no plans to develop interagency doctrine, but some shared training and mission preparation includes civilians, and military training exercises often contain stabilisation elements.

In practice, many of the civilians employed in CA-related positions in Helmand have **a reserve officer background** and are thus able to liaise easily with the military component. However, **military and CA operational and strategic learning have been hampered by a lack formal systems and a low**

degree of strategic reflection (Søby & Salling Larsen, 2010). Regarding military capability planning, CA issues do not seem to affect prioritisation except that materiel for international operations has either been acquired to serve directly in stabilisation missions (such as Mine Resistant Vehicles for Afghanistan) or is required to be multifunctional as future mission preparedness must include the full spectrum of operations.

In 2013, Denmark published a new **policy for stabilisation in fragile states**, bringing renewed attention to 'upstream' conflict prevention rather than 'downstream' post-conflict stabilisation. The new policy document emphasises the continued utility of CA and WGA and is the conceptual framework for the FSF (Ministries of Foreign Affairs, Defence and Justice, 2013).

II.1.3 Internal challenges and initiatives

In Denmark, domestic security related policies have in the period since the 9/11 attacks in the United States been dominated by means to respond to to international terrorism and new risks and threats such as those related to cyber security and other critical infrastructure. In this domain too, the new challenges have presented difficulties to the existing administrative division of labour, resulting in lengthy decision-making processes concerning certain reforms and unsettled issues regarding others.

After the Cold War, the Danish approach to emergency management was reformed as the civil defence organisation and the municipal fire departments were merged under one **single catastrophe preparedness organisation**, administrated by the Ministry of the Interior. Following the renewed focus on man-made catastrophes after 9/11, the government decided to move the Danish Emergency Management Agency (DEMA) under the purview of the MOD in 2004 (MOD, 2004b).

Continuous reforms since the Cold War have meant that the domestic operative structure of Danish emergency management now resides **at the municipal level, supported by five national-level centres**. In keeping with both the historical local roots of disaster response and the international standard all-hazards approach, Danish emergency management policy has traditionally been organised around **a principle of 'sector responsibility'**. This principle emphasises that higher-level organisations such as DEMA primarily help develop the general framework for preparedness plans, whereas concrete plans are developed and implemented at the local level (municipalities) there. This entails risk profiling and establishing a concomitant level of service. Following international trends, this approach was complemented by **a national vulnerability analysis** in 2005 with subsequent annual updates. In the same vein, the EU increasingly requires national-level reporting on, for example, (European) critical infrastructure. Conceptually, this introduces the idea of a new internal security policy prioritisation and potentially challenges the sector responsibility principle (Breitenbauch, 2012).

In a foreshadowing of the current WSA, Danish civil defence and emergency management had involved the private sector through the sector responsibility principle already during the Cold War. The **'Private Sector Home Guard'** covers three sectors of 'societal importance', namely energy,

communication and transport. It is a framework in which public and private companies are connected to the Home Guard and emergency management structure through cooperation on planning and education (Home Guard, 2013). In the same way, the fire service and the large role played by the Home Guard especially in maritime responsiveness is to some extent based on voluntary or semi-voluntary work.

In emergency management policy, the shift of DEMA to the MOD has meant that the **resources of DEMA are increasingly being leveraged in an international context** as one tool among others in the activist foreign policy tool box. Support to international disaster response often happens through multilateral cooperation institutions like the EU and NATO, necessitating planning and training for international interoperability. At the same time, Danish defence has examined ways in which defence assets can be used in international disaster response (just as they are in domestic situations), thus pointing to **a general emphasis on employing state capabilities in a WGA to foreign policy in a broad sense**. Moving DEMA under the purview of the MOD appears to have enhanced this connection in both directions, even if the underlying organisational cultures have not shifted much towards each other.

In addition to this, **cross-cutting issues such as cyber security** have proven to be difficult to resolve without further coordination among political actors. It took more than seven years to establish the Danish computer emergency response team (GovCert), which was founded in 2009 as part of the MOD to replace the former complex network of cooperation among a host of agencies (the predecessor, DK Cert, grew from research and education network protection and was located under the Ministry of Education). The slow implementation of Danish GovCert is an example of the relatively low degree of effectiveness of whole-of-government efforts in Danish central administration. Moreover, the location of GovCert under the MOD, in spite of the relatively limited military role in cyber security, emphasises the ambiguities of Danish security policy in the post-9/11 world.

A final example, beyond the MOD sphere but still related to 'hard' security issues concerns the challenge of international terrorism and the link between domestic groups and individuals, and the larger scenes abroad. Danish FSF whole-of-government approaches to stabilisation in e.g. Eastern Africa include anti-radicalisation programmes, and the Danish Police's Security and Intelligence Service (PET) has partnered with Kenyan authorities (Danish Security and Intelligence Service, 2012).

The transnational character of the threat has meant a new international role for PET, a role which is then also a building block in the formal whole-of-government framework. These new possibilities and tasks for PET, including efforts abroad, have been accompanied by a substantially larger budget. In 2007, the **Centre for Terror Analysis** was founded at PET including a small regular PET staff and 'up to 15' rotating representatives from the Defence Intelligence Service, MFA, PET and DEMA (Danish Security and Intelligence Service, 2013). The new tasks have at the same time raised some questions of principle about oversight and parliamentary control which are as of yet unsettled. The political appetite to address this continuously worrying issue has so far appeared to be stronger than the interest in transparency – as illustrated by the controversy

surrounding the recent case of a former intelligence asset who was instrumental in providing the United States with targeting information on Anwar Al-Awlaki in Yemen.

II.1.4 The potential cost of flexibility

The new array of security-related tasks since the turn of the millennium ranges from post-conflict stabilisation and conflict prevention to domestic critical infrastructure, including the organisation of cyber security and the issue of dealing with terrorism in networks that cut across the domestic-international divide. The traditional division of labour in the Danish central administration has been challenged to respond quickly and effectively in this context, especially to such issues that cut across the normal areas of ministerial competence. Generally speaking, **change has been slow and shallow**. Mostly, this can be explained by the **bureaucratic culture** of the Danish central administration. Relying **on the principles of flexibility and informality**, the traditional culture has promoted effective administration inside ministerial organisations. But these same virtues have fared less well when challenged to deliver effective coordination across organisations, exactly because of the lower degree of formalisation preferred, which includes a reticence to establish new, and especially cross-cutting institutional structures.

The transformation of the new challenges -- such as stabilisation operations or cyber security -- into effective institutionalised tasks and processes also seems to be harder to bring about because there is a **relatively low degree of formal learning within the system**. Permanent or long-lived inter-ministerial committees are little used in Denmark, perhaps also because of the small size of the administration. The trend is for ministries to prefer to **keep decision-making structures in-house**, especially in the case of the MFA. The MFA guards its monopoly on the right to lead/coordinate all Danish external relations with great vigour. As it is itself a relatively large organisation, the most important turf wars take place inside the MFA rather than between ministries.

One exception is the **slightly changed role of the Prime Minister's (PM) cabinet**, which since the millennium and depending on the personality of the PM and on the subject, has taken more of a lead in foreign policy subjects. The MFA's formal lead is challenged now and then when policy subjects appear that are not evidently entirely within its purview, such as the preparations for the 2009 UN environmental summit (COP 15), where both the PM's cabinet as well as the Ministry of the Environment played a large part. In spite of this, the PM's cabinet has not moved forward substantially toward a role of actively coordinating these new cross-cutting challenges - e.g. in a national security strategy (Breitenbauch 2008).

In sum, **a set of mechanisms has been established which has furthered the ability of the Danish government to monitor, implement and plan whole-of-government policies**. As a result, Danish government efforts to address the new cross-cutting challenges have been improved over the period in question. Appraising this situation from a positive point of view, the **instinct to prefer existing arrangements** and eschew new bureaucratic tasks and structures can, of course, also be interpreted as **a sign of frugality and as a preference for the cost-effective solutions that can be found in the existing structures and**

processes. The changes that have been instituted as part of the reaction to the challenges have been rather slow in coming, however. And when they have come, a critical look would sometimes assess them as superficial, such as in the case of the understaffed stabilisation secretariat.

The Danish central administration and its agencies **have been pressed to identify and implement effective processes and institutionalised approaches to comprehensive approach and whole-of-government mechanisms both at home and abroad**. As a consequence of the relatively weak institutional response to cross-cutting challenges that require extensive coordination, this is still a weak spot for the Danish government. Apparently too small to establish formalised cross-cutting coordination and implementation, but big enough to be stove-piped, the changes implemented in Danish central administration appear to be relatively minor. This points to a need for continued attention to the strengths and weaknesses related not only to the formal institutionalised approaches, but also to the role that the bureaucratic cultural preference for flexibility and informality plays with regard to inter-ministerial coordination and cooperation in Denmark. The 2013 stabilisation policy document is one example of a forward-looking attempt to keep forging a unity of perspective and action across all Danish actors, demonstrating the continued salience of the issue.

II.2 Finland[4]

II.2.1 Background

Collaboration between different government and other actors to guarantee the security of the country has long roots in Finnish history. The Second World War was not only about fighting against the enemy in trenches, but also about marshalling the totality of a small country's resources and focusing them on the survival of the nation. This tradition has been carried on, providing the basis even in Finland today of how to prepare for and manage crises facing Finnish society.

For a long time, the emphasis was on how to best use society's capabilities to improve and support Finnish military defence. Reflecting this, the committee established to identify, coordinate and use all society's resources to this end was called the Security and Defence Committee. Appropriately, the Committee secretariat was located in the Ministry of Defence.

It was only in the 1990s that a new approach began to emerge. The special needs of military defence continued to be recognised, but it was also understood that a myriad other challenges and threats are more relevant than the threat of war in people's everyday lives. Cross-border threats such as terrorism, organised crime, trafficking in drugs and humans, infectious diseases, environmental threats, disruptions in energy supply and, last but by no means least, cyber-attacks threaten to disrupt the daily lives of the citizens, and have to be countered and their effects mitigated. Often these global threats are multidimensional and interconnected, and require the use of a wide range of instruments.

[4] By **Dr Pauli Järvenpää**, Senior Research Fellow, ICDS (pauli.jarvenpaa@icds.ee)

II.2.2 Key concepts

The new approach was evident in the Government Resolutions of 2003 and 2006 on Securing the Functions Vital to Society, as well as in the 2009 Finnish Security and Defence Policy Report ('Defence White Book'), where the principles, objectives and implementation criteria for Finland's security and defence policy were outlined. The Government Resolution of 2010 ('Security Strategy for Society') and the 2012 Defence White Book further elaborate the new comprehensive approach. It is still further refined in the 2012 Government Resolution on Comprehensive Security and the 2013 Government Resolution on Finland's Cyber Security Strategy.

In Finland, the critical objectives of **'comprehensive security'** are defined as follows: 'The most important tasks of Finland's foreign, security and defence policy are to safeguard national sovereignty, territorial integrity and basic values; to promote the population's security and well-being; and to maintain the functioning of society' (Finnish MOD, 2010). The measures taken under the principle of comprehensive security **aim to secure the vital functions of society in a cooperative effort in which the state and municipal authorities, non-governmental organisations and business community collaborate with each other**. The aim is to secure the functions vital to society under all conditions, and the main principle is that security in society builds on the arrangements made under normal conditions.

A Government resolution from the year 2010, 'Security Strategy for Society', provides guidelines to all ministries, to regional and local administrations, and to the rest of the society, for achieving these goals. The Strategy is based on 'a comprehensive concept of security' and covers the **preparedness of society and crisis management under both normal and emergency situations**. It provides guidelines to the authorities in public administration, the business community and non-governmental organisations, and harmonises their preparedness planning. Ministries are responsible for the overall preparedness in their administrative sectors, as well as for overseeing the related research, guidance of activities and legislative measures on the basis of the Strategy.

The Strategy aims to provide guidelines for 'safeguarding functions that are vital to society in all situations' (Finnish MOD, 2010: 3). Such functions, according to the Strategy, are the following (ibid, 16):

- Maintenance of State functions,
- Maintenance of international activities,
- Safeguarding of defence capability,
- Maintaining internal security,
- Securing the functioning of the economy and the vital infrastructure,
- Safeguarding the population's daily needs and capability to function, and
- Supporting the population's psychological resilience to crises.

II.2.3 Threat scenarios

In the Strategy, threat scenarios are divided into 'threats' and 'disturbances' (ibid, 13-15). Disturbances refer to a threat or an incident which

endangers, at least momentarily or in a regionally limited way, the security or functioning of society or the livelihood of the population. Disturbances may occur both in normal conditions and in emergency situations. The systems and preparedness measures built for normal conditions provide the basis for actions taken in emergency conditions. Conversely, the systems created for emergency conditions must be available to manage disturbances under normal circumstances.

The threat scenarios used in the Strategy for securing the functions vital to society are the following:

- Serious disturbances in power supply,
- Serious disturbances in telecommunications and information systems (e.g. cyber threats),
- Serious disturbances in transportation and logistics,
- Serious disturbances in public utilities,
- Serious disturbances in food supply,
- Serious disturbances in financial and payment systems,
- Disruptions in the availability of public funding,
- Serious disturbances in the health and welfare of the population,
- Major accidents, extreme natural phenomena and environmental threats,
- Terrorism and other criminality that endangers social order,
- Serious disturbances in border security,
- Political, economic and military pressure, and
- The use of military force against Finland.

II.2.4 The main actors and their responsibilities

In Finland, comprehensive security has been **developed in concert with the authorities, the business community and non-governmental organisations**. Cooperation between these different levels of actors has provided a baseline for contingency planning, the division of roles and responsibilities and the practical measures for implementing policies.

The President of the Republic heads Finland's foreign policy in cooperation with the Government. For countering emergencies, **the Government** is responsible for national preparations and may be authorised to use the additional emergency powers provided in the Emergency Powers Act. This is subject to a parliamentary decision. According to the Emergency Powers Act, the Government would introduce the statute on implementing the Emergency Powers Act after having concluded with the President that the country faces emergency conditions. The final decision, however, is in the hands of the Parliament.

The Government directs, supervises and coordinates the securing of functions vital to society. Each ministry does the same within its respective administrative sector in its role as the **'competent' ministry**. The joint meeting of the President and the Cabinet Committee on Foreign and Security Policy discusses important aspects of foreign and security policy, included salient issues concerning Finland's military defence and comprehensive security. The ministries

cooperate with each other as necessary, under the leadership of the competent ministry.

The **Permanent Secretaries** in each ministry have the task of directing and supervising the activities of their respective ministries. Each ministry nominates a **Head of Preparedness**, who assists the Permanent Secretary in the implementation of preparedness tasks. The **Meeting of Permanent Secretaries and the Meeting of Heads of Preparedness** are permanent cooperation bodies, in which preparedness issues and their coordination are discussed and handled. Heads of Preparedness are assisted in their tasks by **Preparedness Secretaries**, nominated in each ministry.

Two ministries have a special position in this system. The **Ministry of Defence** is **responsible for coordinating all comprehensive security activities**. This involves **synchronising such activities in the public sector** (government, state authorities and the municipalities), in the **business sector**, and **in the voluntary sphere** (i.e. activities by Finnish citizens through non-governmental organisations) in order to maintain the functions vital to society under all circumstances. The **Security Committee** (before February 2013, the Security and Defence Committee) assists the Ministry of Defence in these tasks. The Committee is historically part of the Ministry of Defence structure, but it **serves the government and all the ministries** in preparing, coordinating and implementing comprehensive security measures.

The other ministry with an overarching general task in the field of comprehensive security is the **Ministry of Finance**. It is responsible for the general guidance and development of common information systems and networks in Finland. It is also responsible for the general guidance and directing of information society and ICT preparedness in the public sector.

Various levels of **regional administration** also have roles in comprehensive security activities. Regional administration was reorganised in 2010, when the **Regional State Administrative Agencies (RSAA)** and the **Centres for Economic Development, Transport and the Environment (CEDTE)** were established. The former are responsible for coordinating preparedness in the regions, coordinating preparedness planning, supporting preparedness planning in the municipalities, and organising preparedness exercises in the regions. Regional preparedness committees were established for these purposes. The CEDTE are responsible for implementing and developing preparedness and crisis management measures in their areas in connection with the environment and natural resources, traffic and infrastructure, business activities including agriculture, the use of the workforce, immigration, education and culture.

One further level of preparedness planning takes place in the **municipalities**, where the responsibility for organising basic services and other functions vital to society lies. The obligation of the municipalities to prepare for emergency conditions comes from the Emergency Powers Act. Furthermore, the **business community** is an essential partner in the municipalities in preparing to protect the vital functions of society through effective cooperation.

The Ministry of Employment and the Economy is responsible for developing security of supply. The Finnish organisation for security of supply consists of the **National Emergency Supply Agency**, which is a public body

subordinate to the Ministry of Employment and the Economy, the Council for Security of Supply and Infrastructure, and the security of supply sectors and pools, which act as permanent co-operation bodies.

The National Emergency Supply Agency is responsible for the tasks related to the **coordination, development, and maintenance of security of supply**. Its instruments include the emergency stockpiling of critical products, legislation on preparedness and financial and economic policy, and the voluntary participation of critically important companies and organisations. This sort of preparedness planning is a good example of **successful voluntary public-private partnerships.**

Last but not least, there are myriad **non-governmental organisations (NGOs)** that have their vital role in providing everyday security and in improving individual citizens' crisis resilience. Such organisations include voluntary fire brigades, local Red Cross organisations, farmers' associations, and sports clubs, just to name a few. By supporting the government authorities, they play an important role in, for example, search and rescue, civil defence and fire-fighting, voluntary military defence, first aid and psychological support functions. They are also a significant actor in providing early humanitarian aid to crisis areas, at home and abroad.

II.2.5 The key role of the Security Committee

The task of the Security Committee, still located in the Ministry of Defence, is to assist the Government and various ministries in matters pertaining to comprehensive security. It also coordinates preparedness issues related to comprehensive security. **In case of disturbances or emergencies, the Committee will act as a specialist body**. The Committee is a non-permanent body of government officials and experts, nominated by their ministries or agencies. It meets regularly, usually once a month, to deal with issues within its competence. In its present form, the Committee started its work on February 1, 2013, when it replaced its predecessor, the Security and Defence Committee. It has 19 members and 3 permanent experts. **Finland's Cyber Security Strategy**, produced under the auspices of the Committee in 2013, is a good example of its work.

The Committee is chaired by the Permanent Secretary for Defence, the highest non-political official at the Ministry of Defence. The Deputy Chairman is the State Secretary from the Prime Minister's Office. There are members, all at the level of Permanent Secretary or equivalent, from the: Office of the President, Ministry for Foreign Affairs, Ministry of Justice, Ministry of the Interior, Ministry of Finance, Ministry of Education and Culture, Ministry of Agriculture and Forestry, Ministry of Transport and Communications, Ministry of Employment and Economy, Ministry of Social Affairs and Health, and Ministry of the Environment. In addition, the Committee includes the Director General from the Ministry of the Interior, the National Police Commissioner, the Chief of Defence Staff from the Defence Forces, the Chief of the Border Guards, the Director General from the Customs Authority, and the Chief Executive Officer of the National Emergency Supply Agency. The three expert members of the Committee are the State Secretary for EU Affairs from the Prime Minister's Office, the Director of Government Communications also from the Prime Minister's Office, and the Chairman of the National Emergency Supply

Council.The Security Committee is provided with a small secretariat: currently 13 officials, 6 of them permanent and 7 part-time.

II.2.6 Other issues

In the last few years, much attention has also been paid in Finland to the issue of **cyber security**. Finland is one of the most advanced countries in the world in terms of information technology applications in society. Yet, it came as a shock in early November 2013 when the penetration of the Finnish Ministry for Foreign Affairs reporting system by foreign spies over the last four years became publicly known. One of the many results of this attack will be that the legislation that was already in preparation will be speeded and strengthened. Also, the implementation of concrete counter-measures will be accelerated.

The present system of comprehensive security is **tested every four years in a country-wide exercise** called VALHA ('valtionhallinto', or state administration). The latest exercise, VALHA-13, was carried out in 2013.

There is some debate on where the Security Committee should be located. For historical reasons it has always been part of the Ministry of Defence, but some would like to see it located in the Prime Minister's Office. At least for the remainder of the current Government's term in power - until the next parliamentary elections in 2015 - the Security Committee will continue to operate from its present office in the Ministry of Defence.

II.3 The Netherlands[5]

The security policies of the Netherlands place a strong emphasis on comprehensive solutions to external and internal security challenges. The coordinated deployment of instruments available to the government that are relevant to the particular circumstances – the **integrated approach --** is a well-established principle. This section reviews the strengths and weaknesses of the Dutch approach in bringing together various security stakeholders.

II.3.1 Policy framework – not so integrated?

Despite the continuous rise of the importance of the integrated approach in Dutch security thinking, its policy framework remains, by and large, split between external and internal vectors. Externally, the Netherlands directs its actions on the basis of its **International Security Strategy** (ISS), which formulates the Dutch view of the external security environment, establishes the Netherlands' strategic interests in the world and defines the main areas of policy focus. The process of formulating the ISS is led by the Ministry of Foreign Affairs. Internal security is governed on the basis of the **National Security Strategy** (NSS), which lays out the process for assessing internal security risks and threats, defines vital interests in this realm, establishes principles for securing those interests and develops key themes that require action. This process was initially led by the Ministry of the Interior and Kingdom Relations, but after government restructuring was taken over by the Ministry of Security and Justice. In addition, there are policy documents covering either a particular area of institutional responsibility (e.g. the Defence White Paper) or a domain which cuts across

[5] By **Tomas Jermalavičius**, Research Fellow, ICDS (tomas.jermalavicius@icds.ee)

many areas of institutional responsibilities (e.g. the National Cyber Security Strategy). They are all approved by the Netherlands' Cabinet.

The absence of an overarching security strategy, combining and integrating both external and internal vectors, is somewhat **discordant with the Dutch emphasis on integrated approaches**. In fact, the current NSS was drafted with a view that it would include both external and internal security aspects. However, the Ministry of Foreign Affairs eventually opted to stay out of this process and to continue with the ISS as a separate framework, probably and indication of the MFA's wish to protect its lead in external relations. Recently, the Government resolved that the two security policy vectors should be brought under a single overarching document, but the latest iteration of the ISS ('A Secure Netherlands in A Secure World') was published in 2013 as the usual stand-alone document.

In spite of this, the Dutch security policy expert interviewed for this report saw a **degree of convergence and similarities between the ISS and NSS**, as the interests outlined in both overlap (e.g. economic security features in both documents; internal social and political stability in the NSS echoes the international legal order in the ISS; defence of national and allied territory in the ISS reflects territorial security as a vital interest in the NSS). Issues and opportunities flowing from membership of the EU also cut across both strategies, raising further questions as to whether the separation of internally and externally oriented security policy frameworks is reasonable. There is some feeling in the Netherlands that this will have to be changed, although the change will be slow due to the habits of the ministries and departments, which are eager to protect their turf.

II.3.2 Integrated approach as a key concept of Dutch security policy

Despite the separation of the internal and external security policies, both the ISS and NSS place a strong emphasis on **integrating various tools of national power to manage contemporary security challenges**; indeed, one of the policy focus areas of the ISS is titled 'integrated approach'. According to the document, 'Recent experiences in Afghanistan, Bosnia, Iraq, Kosovo and Libya have shown that intervention is effective only if the instruments of defence, diplomacy, development cooperation, the police, the justice system and trade are deployed in a coordinated fashion' (The Netherlands Ministry of Foreign Affairs, 2013:16). It further notes that, 'An integrated approach also allows better coordination of the activities of Dutch military personnel, police officers, lawyers, businesses, civil society organisations, civilian experts and diplomats in conflict zones' (Ibid). In some specific areas such as cyber security, energy, resource availability and counterpiracy, the ISS policy focus is set on engaging the private sector as a critical stakeholder in security.

Similarly, the NSS also calls for a joined-up, integrated and coherent approach to national security. It states that:

> Naturally governments and private parties are already active in strengthening security. In order to be able to effectively direct these efforts, now than ever cooperation is needed between all organisations that are responsible for national security: national government, local authorities, social organisations and the business community. An approach that guarantees integrity and

> coherence across security sectors is essential. (The Netherlands Ministry of the Interior and Kingdom Relations, 2007: 12)

Just as the ISS, the NSS also points out that the private sector has very important responsibilities in safeguarding society's critical functions in crisis circumstances and in responding to threats. This particularly pertains to information and communication, energy and other critical infrastructure (NSS, 2007:32).

This framework lays the ground for practical steps to develop methodologies, processes and mechanisms aimed at integrating various instruments, even though it is acknowledged that the precise mix of instruments and their application will always vary depending on circumstances.

II.3.3 Implementation mechanisms

In implementing the integrated approach, both the ISS and NSS stress the importance of mutual awareness, and joint threat assessments, analysis, planning and learning mechanisms. For instance, the ISS (The Netherlands Ministry of Foreign Affairs, 2013: 17) states, when describing its policy focus on an integrated approach:

> Collaboration begins in The Hague. Government ministries coordinate their activities among themselves and with external actors such as civil society organisations. An integrated approach to planning is also needed. Joint analysis involving all relevant ministries and organisations is an important first step in the process. Once the decision has been taken to provide a contribution, it is vital to establish the baseline situation. Any plan for transferring responsibility to the local (and, where necessary, the international) community must be based on analysis and measurement. Finally, a thorough joint evaluation allows lessons to be learned and put into practice, as happened after the missions in Uruzgan and Kunduz.

The NSS (The Netherlands Ministry of the Interior and Kingdom Relations, 2007: 10) likewise states that, 'in order to enable an integral approach, all parties involved must know and respect each other's role in strengthening national security, follow a shared doctrine, align their working methods to each other and be connected to the same communication network.' This is reflected in the four **principles of authority and control** laid out in the strategy: **clear role division and role consistency**; ***unité de doctrine***; **alignment of working methods** (including decision-making processes, communication strategies, synchronisation of planning and regular joint exercises and training); and a **uniform information network** (Ibid, 31-32).

The ISS statement has been informed by Dutch experience in operations, particularly in Afghanistan. Indeed, the pressure for the capital to become more systematic, coherent and comprehensive in its policies and practices grew from the bottom, from the Dutch-led task forces on the ground in Afghanistan. Initially, a **Collaborative Decision-Making (CDM)** model, which aimed to involve all relevant actors in the area of operations and tie them together in a coherent manner in all relevant dimensions (political, social, economic and security), was drawn for the task force in Uruzgan (see Spoelstra et al, 2010). After a few years, a more elaborate and updated version of the model was applied to campaign planning in Kunduz (van Bemmel & Eikelboom, 2010). This is now being turned

into an even more comprehensive generic model, which would be applied by the government in The Hague to plan all operations abroad.

In the process of developing this model, significant **differences between the military and civilian approaches to mission planning** had to be bridged. According to one interviewed expert, the military usually envisage a desired end-state and draw a number of courses of action to achieve it; civilian organisations, particularly diplomats, usually envisage a range of acceptable outcomes and navigate towards them within a certain bandwidth which constrains freedom of action. The CDM has proved that the two approaches can be reconciled through systematic and evidence-based development work, and can be successfully applied in operations.

Although the CDM model has yet to be elevated from the tactical and operational levels to the strategic-political level, several institutional arrangements are already in place to promote the WGA in operations outside the Netherlands. For instance, the MFA has a **coordinator for security issues and comprehensive approach** in its Stabilisation and Humanitarian Aid Department. At the political level, there are **steering groups on military operations and civilian missions**, which bring together senior defence, foreign affairs, finance, economy and justice officials (Wittkowsky & Wittkampf, 2013:2). Some interviewed experts, however, believe that the discussions in these formats are too tactical and operational, seldom touching upon more fundamental strategic issues.

There are currently no guidelines for an integrated approach or doctrine for inter-agency training to support involvement in international operations, although some exercises address issues of collaborative decision-making and inter-agency interactions. However, according to one interviewed expert, operational experiences in Kunduz led the Dutch police and military police, who had to collaborate a lot in the area of operations, to conduct more joint exercises and to seek to align their doctrines. It is quite likely that, once the CDM model has spread and become established practice, a doctrine or a set of guidelines for the whole-of-government integrated approach towards international conflicts will eventually be formulated.

The NSS outlines the main building blocks for whole-of-government activities. These include, as stage one, **government-wide analysis**, i.e. **strategic foresight, thematic in-depth studies and scenarios, short-term horizon scanning and national risk assessment**. In stage two, **strategic planning** is conducted, where planning assumptions are made, the assessment of the capabilities required to meet the identified threats is undertaken, and where matching of those requirements against existing capabilities is performed. In the final stage, or **follow-up**, various policies, legislation and measures are enacted to implement the strategic plans (NSS, 2007: 21).

There are also **institutional mechanisms** to support the implementation of the NSS. For instance, nine ministries cooperate in implementing an integrated **Critical Infrastructure Protection (CIP)** programme, which is also closely linked with the inter-agency **Threats and Capacities (T&P)** programme, responsible for national risk assessments as well as capacity building. In this, the ministries are supported by the informal **Strategic Council for Critical Infrastructure Protection**

(SOVI), which is a **public-private partnership of CIP stakeholders**. Knowledge and information exchange, networking and advice are provided by the **National Advisory Centre for the Critical Infrastructure (NAVI)**. There are similar arrangements ('issue based units') in other fields to facilitate the integration of various internal security stakeholders and their coherent actions, including the **National Crisis Centre (NCC)** responsible for national crisis response; the **National Coordinator for Counterterrorism (NCTb)**; and, most recently, the **National Cyber Security Centre** in the area of responsibility of the Ministry of Justice and Security.

The **civil-military dimension** is an important constituent of the Dutch integrated approach. Ten years ago, the Netherlands Armed Forces were declared a **strategic partner of the civilian security** organisations. This is in line with core missions, which encompass territorial defence (e.g. against terrorist attack) and assistance to civil authorities in the event of emergencies and during crises. A **catalogue of military capabilities** available for managing civil contingencies was developed by the armed forces and included such capabilities as CBRN, EOD, engineering, transportation and medical capabilities, naval vessels, radars, and UAVs. Some **joint civil-military training facilities** (e.g. in CBRN) were also set up (The Netherlands Ministry of Defence & The Netherlands Ministry of the Interior and Kingdom Relations, 2007).

Domestically, however, the integrated approach, suffers from a number of **shortcomings**, which will take time to address. According to the interviews, chief among these are:

- Although national risk assessment (the first phase of the NSS process) is methodologically one of the most sophisticated and elaborate among such processes in the world, the **strategic planning phase** is rather weak. Organisations seldom conduct generic planning of capabilities together or include one another's needs in their own planning considerations.
- The **civil security sector at the local, regional and national levels is rather fragmented**, making it difficult for the defence organisation to deal with a broad variety of stakeholders who often have conflicting requirements. An on-going process of centralisation in managing some of the civil security functions might help to rectify this in the future.
- **Awareness of the capabilities** of the civil security sector is limited on the defence side. There is no corresponding catalogue of civilian capabilities available to the defence organisation.
- The defence organisation is still too insular, and does not see itself as an integral part of the internal security apparatus. With its primary focus on expeditionary operations, it is less enthusiastic about its internal security functions.
- Crisis management structures are still too **stove-piped**, meaning that the civil-military interface is not as responsive as it could be and can be hampered by multi-layered and stove-piped lines of communications between the authorities at different levels (e.g. for a request to go from a mayor to a local military unit commander, it has to go up the civilian

chain of governance and then, having passed from the civilian to the military system, return down the military chain of command).

- Various civil-military exercises demonstrate **persistent problems with coordination, interoperability, doctrinal void or disharmony and too divergent processes**. This indicates that the goal of the NSS to achieve more integration is still some way off.

II.3.4 Cultural aspects

One of the key features of the Dutch culture of political and governance is the so-called **Polder Model**, 'which favours consensus and cooperation irrespective of individual rank', and which 'builds on pragmatic trial and error processes' (Wittkowsky & Wittkampf, 2013:2). This culture quite strongly underpins the institutional and personal interactions between security and defence stakeholders (public and private), although examples of some ministries still going ahead with separate strategies or the challenges of civil-military interaction demonstrate that it has its limits. Nonetheless, the bottom-up emergence of the CDM model serves as an illustration of how integrated approaches can be advanced through trial, experimentation and error as well as through a cooperative attitude of the involved stakeholders.

The consensual and democratic nature of Dutch political and governance culture is also **averse to dominant institutional or personal actors in decision-making**. This, according to one interviewed expert, may explain why the Netherlands lacks a powerful Prime Minister's office which could act as a strong and active integrator of various strategies, policies and planning processes. Such a role for the PM's office may nonetheless emerge in the future, under the continuous pressure of cross-cutting security issues and operational challenges. It will, however, be a slow process and will have to take into account the diversity of security stakeholders, and upon the consensual culture of the Polder Model.

II.4 Sweden[6]

II.4.1 Background

During the Cold War, Sweden employed a total defence concept which had the purpose of defending the nation against an armed attack. The concept aimed to coordinate the activities of all relevant government authorities to support the armed forces. In the early 1990s a vast number of agencies tasked to coordinate activities in the field of civil defence, psychological defence, self-sufficiency and ensuring the vital functions of Swedish society remained. The extent of these activities can be gleaned by recalling that Sweden had decided to remain non-aligned in peace time with the aim of being neutral in times of war. Thus there was no possibility to rely on allies – Sweden would depend entirely on its own resources.

In the mid-1990s it became obvious that the Cold War was over and that the military threat was gradually disappearing. A major threat and risk

[6] By **Martin Hurt,** Deputy Director, ICDS (martin.hurt@icds.ee)

assessment study was launched by the Government, following which focus shifted from countering military threats to planning for civil emergencies, which had so far seen only limited attention. Previously it had been assumed that if the civil authorities were able to mount a credible civil defence system to support the armed forces, they would also be effective in the case of emergencies, crises and disasters. All contingency planning was cancelled and so were most crisis management exercises. Some organisations were merged, others were replaced by newly established structures of which a couple were disbanded after only a few years (Werger, 2013).

The 2004 tsunami in Thailand, where 543 Swedish citizens lost their lives and around 1500 were injured, was a wake-up call for the political leadership (2005 års katastrofkommission, 2005: 102). It was suddenly realised that even though many agencies were engaged in the aftermath, no agency had the sole responsibility of creating an overview of the situation (Werger,2013).

In 2006, new legislation came into place to task the ministries, other government authorities and regional and local administrations to take action in order to ensure that they were capable of fulfilling their tasks in times of crisis and other emergency situations. Regional and local administrations should, through these activities, achieve the capability to conduct civil defence.

A central element of the new regulation is the areas of cooperation[7] within which government authorities are required to conduct planning in order to be prepared for crisis and other emergency situations (Riksdag, 2006:942, §8). The Swedish Civil Contingencies Agency (abbreviated MSB), established in 2009, supports this coordination by providing methods and networks for the government authorities during extraordinary events.

A study about the need to create a national crisis management function at the Prime Minister's Office was conducted in 2007, leading to a new office being set up: the Crisis Management Coordination Secretariat (Werger, 2013).

The 2008 war in Georgia led the Government to task the Swedish Armed Forces to prepare contingency plans for the military defence of Sweden, which had not been done since the 1990s. But it took five more years – until Spring 2013 - for the Government to task MSB to also prepare contingency plans for civil defence, including private companies (Werger, 2013; Hedström, 2013).

However, it will not be possible to rebuild the Total Defence system that existed during the Cold War as the military, civil society and the threats themselves have changed (Werger, 2013; Hedström, 2013). The Armed Forces are no longer primarily designed to deploy a large reserve force in order to repel an armed attack against the whole of Sweden, but to participate in expeditionary operations with high readiness units manned with all-volunteer contracted personnel.

Civil society has also changed radically:

- **Internationalisation** means that the Swedish economy is now intertwined with that of the rest of the world. Sweden is no longer self-sufficient regarding energy, telecommunications, transportation, commodities or

[7] The six areas of cooperation are: infrastructure; transport; hazardous substances; economic security; protection and rescue; and healthcare.

food supply. Sweden lacks control over the flows of these resources, which also makes it no longer possible to plan for security of supply in the same way as earlier.

- **Privatisation** has meant that important infrastructure, such as harbours, airports, electricity and communication networks no longer belongs to the state and that ownership is more diverse than earlier. Foreign ownership has also increased drastically.
- **Efficiency** improvements in terms of 'lean production' and 'just in time' have led to radically decreasing stocks. Previously existing buffer stocks that were intended to be used in times of crisis or war have been eliminated. This applies also to the public sector and even healthcare depends nowadays on very small margins. The only stocks that exist include fuel and medicine (Werger, 2013).
- Development of **technical infrastructure** has led to increased dependence on a robust supply of electricity and the availability of telecommunications.
- Development of **information technology** has created new problems regarding dependence and vulnerability. Internet and social media has created new challenges for contingency planning, e.g. cyber-attacks.

These changes in society mean that old concepts are no longer valid and need to be abolished (FHS, 2013: 4-5).

In December 2012, the Swedish National Defence College was tasked by MSB to propose an action plan for the creation of a new civil defence system to be integrated into modern society. A draft report highlighted the previous (1990s) legislation's focus on civil defence as an **activity** and compared this with the more modern approach to consider **civil defence as a capability** (Ibid, 6).

II.4.2 Key concepts

While the **total defence concept** is still valid and has not been erased from the legislation, current policy documents no longer use this term. The latest report presented by the joint parliament-government committee on defence policy (Försvarsberedningen) on 31 May 2013 refers to the **comprehensive approach to security** (Regeringskansliet Försvarsdepartementet, 2012: 222). The report states that 'Security is a wider term than just protection of own physical territory.

The joint committee also states that 'interaction between civil and military crisis management actors can deepen further. This is applicable both for military support to other elements of society and the civil authorities as well as the support made available by those civil authorities to the Armed Forces to enable them to fulfil their tasks.' (Ibid, 225).

II.4.3 Underlying principles

The Swedish crisis management system is guided by three underlying principles: the principle of responsibility, the principle of proximity and the principle of equality (MSB, 2011:11):

- The **principle of responsibility** means that whoever is responsible for an activity in normal conditions should maintain that corresponding responsibility, as well as initiating cross-sectoral cooperation, during major emergencies (Ibid, 24).
- According to the **principle of proximity**, a crisis is to be handled in the area where it takes place, and be managed by those most closely affected and responsible. Crisis management should only be referred to higher levels if it is considered necessary (Ibid).
- The **principle of continuity** means that an organisation's activities and location should, as far as possible, be kept the same during a crisis. Changes to an organisation should be no larger than is necessary to handle the crisis (Ibid).
- A further principle that affects crisis management is the **principle of financing**. The state has by law tasked municipalities to fulfil certain functions during civil contingencies and when the readiness level has been raised. According to this principle, the state also has to provide funding to enable the municipalities to fulfil these tasks (MSB, 2013: 1).

There are of course exceptions to these formal principles. The principle of proximity is overruled in the case of a nuclear accident when the crisis is handled not according to its geographic location but by the agency that has the capability to handle nuclear accidents. By law there is, however,an exception from the principle of continuity in that municipalities are required to set up a temporary crisis management committee in the case of an emergency (such committees do not exist under the usual circumstances) (Hedström, 2013).

There is also an additional, informal principle: the **principle of solidarity**. According to this, security shall be provided together with other nations as expressed by the Swedish Declaration of Solidarity. This applies to EU members, and to Norway and Iceland (FHS, 2013:6).

The tasks and objectives for Swedish Civil Emergency Planning (CEP) during peacetime emergencies are to:

- minimise the risks and consequences of major emergencies;
- advance and support societal preparedness for emergencies;
- coordinate across and between various sector boundaries and areas of responsibility.

The extended international task of Swedish CEP is to increase capacities for dealing with a wide spectrum of situations and emergencies, ranging from international confidence building measures to coordinated crisis management in complex emergencies.

II.4.4 Legal aspects

Sweden's legal architecture is partially obsolete since some elements of legislation date from the early 1990s, although new laws have been adopted later to reflect developments in specific areas.

According to the Law on Total Defence, adopted in 1992 (Riksdag, 1992:1403), Total Defence is defined as activities undertaken in order to prepare Sweden for war. **Total Defence consists of Military Activities (military defence)**

and Civil Activities (civil defence). In times of war, civilian agencies and other organisations support the Armed Forces. In peace time, civil defence includes activities in local municipalities, and on the regional and national levels aimed at raising society's capability to resist an armed attack (MSB, 2012b).

The law defines various **levels of readiness**. Once the readiness level has been raised, local municipalities and county councils (Landsting) as well as those private companies and organisations that are also committed to operate during war, must take action with regard to planning their activities and managing their personnel and other resources that will enable them to fulfil these commitments. When the highest level of readiness is proclaimed, Total Defence is equal to all activities that society undertakes (Riksdag, 1992:1403).

MSB uses the term **civil protection** that is defined (MSB, 2012:45) as public safety in the form of:

1. protection from incidents and accidents, including everyday accidents;
2. emergencies and disasters;
3. civil defence.

When analysing the existing legislation, it is obvious that it has been gradually developed over the last 20 years. The Law on Total Defence, adopted immediately after the end of the Cold War, focuses on military threats against the nation and states that the task of civil defence is to support the Armed Forces, not the other way around. Later laws and regulations foresee that the Armed Forces should be able to support civil society during emergencies and disasters. The responsibility for civil emergency planning is managed by three different levels of government – national, regional, and local.

II.4.5 The national level

On the national level, the **Government** has the executive power and governs the nation (Riksdag, 1974:152, Chapter 1, §6). The Government is responsible for issuing policies for crisis management, exercising overall strategic coordination and determining priorities. In addition, the Government is responsible for effective crisis management, relations with the public and media, and international coordination with other nations and organisations. All operational activities are delegated to civil authorities.

Unlike their counterparts in many other countries, Swedish ministers have limited opportunities to take independent decisions. All government decisions are taken collectively by the Government as a whole after the matter has been well prepared and agreement reached. The Prime Minister bears the ultimate responsibility for ensuring that policies are coordinated and follow the same line (the Government at work). Only regarding the Swedish Armed Forces does the Constitution allow the minister in charge (that is the Minister of Defence) to take decisions under the supervision of the Prime Minister (Riksdag, 1974:152, Chapter 7, §3). The Prime Minister chairs Cabinet meetings but has no authority to take decisions in the name of the Government or in any other capacity.

The Prime Minister's Office is headed by the Prime Minister. Attached to the Prime Minister's Office is the **Crisis Management Coordination Secretariat**.

According to the Government Offices of Sweden, the Crisis Management Coordination Secretariat is responsible for

- policy intelligence and situation reporting;
- crisis management and crisis communications;
- analysis;
- being a central contact point at the Government Offices.

The Secretariat's role is to conduct continual policy intelligence activities. It follows events both inside and outside Sweden around the clock. The Secretariat also fulfils an important function by supporting the ministries in their development of crisis management and crisis communication, arranging training and exercises and producing analyses of threats and risks that could affect Sweden.

In a crisis, the Secretariat supports the Government Offices in managing the crisis. Crisis management tasks include raising the alarm and obtaining an overall picture of the situation and a view of the joint impact on society of the individual events. The Head of the Secretariat is also able, if necessary, to start crisis management measures in the Government Offices. After the crisis has been dealt with, the Secretariat has to be able to follow up and evaluate the measures taken (Crisis Management Coordination Secretariat).

The **Ministry of Defence (MOD)** has overall political responsibility for military defence and civil emergency preparedness. Under the MOD, the **Swedish Armed Forces** are responsible for military defence and the **Swedish Civil Contingencies Agency (MSB)** for civil emergency preparedness.

The task of the MSB is to enhance and support societal capacities for preparedness for and prevention of emergencies and crises. When an emergency or crisis occurs, MSB supports the stakeholders involved by taking the measures necessary to control the situation (MSB – Swedish Civil Contingencies Agency). MSB holds a mandate for a holistic and all-hazards approach to emergency management, including the entire spectrum of threats and risks, from everyday accidents to major disasters.

Crisis management at the Government Offices is based **on a joint cross-sector approach.** Every government office is responsible for planning and handling crises within its own area of responsibility. Authorities and agencies at the national level are also assigned complementary tasks by the government during major emergency situations.

Every government agency is also responsible for civil emergency planning in its own area of expertise, and the MSB has the task of coordinating the various stakeholders. This responsibility applies to measures taken before, during, and after the occurrence of emergencies and disasters. All Swedish authorities are obliged to carry out risk and vulnerability analyses in their own areas in an effort to strengthen their own, and Sweden’s overall emergency management capacity (MSB – Swedish Civil Contingencies Agency). Authorities providing vital services must have a point of contact available on a 24/7 basis and also a command and control capability (Werger, 2013).

There is no longer a legal mechanism committing private companies to also operate during war time. During the Cold War, a number of designated companies were tasked with the production necessary for war time needs. These

companies were also responsible for protecting their production facilities. Some only had to increase their production in times of war, others had to switch their production from peace time commodities to meet war time needs (Bergrum.se, 2013). This is again under consideration, as many functions vital for society are today provided by private companies (Werger, 2013).

II.4.6 The regional level

At the regional level, the county administrative boards are responsible for the coordination of civil emergency activities such as exercises, risk and vulnerability analyses. They also act as a clearing house between public and private partners. During a crisis, the administrative boards coordinate the relevant measures with relevant actors. The county administrative boards have overall responsibility for reporting the need for host nation support in the event of a major emergency. Additionally, the county administrative boards also coordinate contact with the mass media during major emergencies, crises, and disasters (MSB – Swedish Civil Contingencies Agency).

II.4.7 The local level

Swedish municipalities have a large degree of autonomy and play an important role in civil emergency planning and preparedness. During a major emergency the municipal executive board is the highest civilian authority within the municipality, and is responsible for all civilian command and crisis management at the local level. Municipalities are supported and assisted in this role by the county administrative boards (MSB – Swedish Civil Contingencies Agency).

II.4.8 Mechanisms used to encourage inter-agency interactions

MSB has, in a study, identified a number of enablers and barriers to inter-agency cooperation. According to military personnel who participated in the study, there are **often fundamental differences between military and civil organisations**, both in domestic and international situations. One important barrier is the **strict tradition of issuing orders in the military, whereas civil organisations are more used to collaborate and cooperate**. 'Operational' organisations, including the military, police and rescue services, are often considered by the military to be clearer and more distinct when compared to colleagues from 'non-operational' organisations responsible for social care etc. Military organisations often face a higher rate of staff turnover due to their rotation system which hampers cooperation with other organisations, where colleagues often work together for many years (MSB, 2007:45).

According to the same study, inter-agency cooperation can be improved by gaining more knowledge about partner organisations and their way of operating, by exchanging liaison personnel and by appointing decision makers with a particular set of personal skills and the ability to identify and accept differences (Ibid, 55).

This suggests that any setting that involves decision makers from a wide range of organisations, be it on the local, regional or national level, can work

effectively only if the parties involved understand the resources available to and limitations of the other organisations.

According to MSB, crisis management is systematically improved by using three different means:

- adoption of new legislation and regulations to convince an actor that he/she **must** act;
- providing economic incentive to make an actor realise that he/she **benefits economically** from taking certain steps;
- educating actors to persuade people to take action because it is **appropriate or necessary**.

The **Swedish National Defence College** is tasked by MSB and the Armed Forces to educate senior decision makers including politicians, civil servants, officers and other leaders from military and civil organisations, including the private sector (Hedström, 2013). This is accomplished through a number of different courses on Crisis Management, from four-day courses for the most senior decision makers to longer, seven-week courses for mid-level decision makers and experts (Bergrum.se, 2013).

Part II Conclusions

In all four countries covered in this report, comprehensive thinking in security affairs emerged gradually and is manifested in a variety of ways. In some cases (e.g. in Denmark), it is oriented more towards external actions, i.e. in conducting complex operations abroad, and has been driven by experiences from such operations. In other cases, it is more domestically focused and driven by the adaptation of internal security systems to the contemporary security environment (e.g. in Finland). But even when comprehensive whole-of-government thinking dominates both external and internal security policy and action, it does not necessarily mean both strands are very well tied together (e.g. in the Netherlands).

All the cases contain many practices worth emulating in Estonia (see 'Key Insights' below), yet they represent different degrees of institutionalising those practices. Historical legacies, institutional inertia, administrative cultures and other factors slow down or even prevent full-fledged and sustained institutionalisation. There are also weaknesses which are yet to be addressed in most of the cases, for instance, lack of effective strategic planning systems to support WGA/WSA, or mature inter-agency learning mechanisms and doctrines.

A striking feature in all cases is the **centrality of defence organisations to the efforts to implement comprehensive security concepts**. This is partly due to their set of missions, which include both external and internal functions and which span the entire spectrum of situations – from peacetime through crises to wars. This often makes them the central hinge on which comprehensive operations rely. It is also partly the legacy of the total defence paradigm, in which defence owned, operated or relied upon the large systems (including voluntary defence organisations) necessary to channel society's resources to support military defence efforts. The challenge is how to build upon this legacy in

creating and running WGA/WSA systems in pursuit of integrated and comprehensive security and defence.

Key Insights from Part II

- **Political consensus** (e.g. in the form of the parliamentary defence agreement as in Denmark) forms an important basis for a sustained whole-of-government and whole-of-society approach to international and national security.
- The **terminology and narrative** employed to describe WGA/WSA should be understandable and not antagonise various security stakeholders such as NGOs, or civilian security agencies (e.g. the Finnish focus on 'resilience').
- **Culture matters**. For instance, a preference for flexibility and informality (as in Denmark) or consensus-building (the Netherlands) are important determinants of the characteristics that WGA/WSA arrangements acquire.
- A degree of **formalisation and institutionalisation** of WGA/WSA, including in inter-organisational planning, decision-making and learning, is necessary to make it work.
- **A set of clear principles** governing the security sector and WGA/WSA (as in Sweden and the Netherlands) is useful in establishing common understanding and managing the expectations between security stakeholders.
- It is necessary to establish **an effective overarching structure** vested with proper authority and supported with the necessary resources (as in Finland) to guide, integrate and oversee the WGA/WSA efforts – ideally, in the prime minister's office.
- **'Issue-based' integrating units** (e.g. for counter-terrorism, critical infrastructure protection, cyber security) are important tools in ensuring broad and comprehensive solutions in addressing those issues.
- Dedicated **budgetary trust funds** for cross-cutting issues that do not fall under the full purview of a particular ministry (as for stabilisation missions in Denmark) provide the necessary financial basis.
- Having **a systematic and methodical approach** (guidelines and toolbox) to monitoring, analysis, assessment and review/learning in managing security (as in the Netherlands) greatly benefits the WGA/WSA.

- Strategic planning of resources and capabilities for WGA/WSA requires **building capacity** for that in the government.
- **Voluntary organisations** make important contributions to WGA/WSA, and using existing home guard structures is an effective way to shape and utilise this contribution.
- **Realistic exercises** including all levels of government and all stakeholders relevant to different crises are necessary to develop WGA/WSA. This can be augmented with a coherent doctrine for comprehensive security missions.

Part III: The 'State of Play' in Estonia – Challenges of Implementing Integrated Defence[8]

Introduction

In this part, the report examines the 'state of play' in Estonia when it comes to implementing whole-of-government and whole-of-society approaches in national security and defence. It mostly focuses on the challenges of putting into practice the concept of 'integrated defence' (also often referred to as 'broad-based defence'). However, it also dwells upon various aspects of wider national security architecture in the country and upon interactions of civil and military stakeholders of security in non-defence contexts (e.g. in civil emergencies). First, it describes the conceptual, legal, institutional setup existing in Estonia; second, drawing upon a series of extensive interviews, it covers the expert opinions on this setup – its strengths and weaknesses as well as practices behind it.

III.1 Background

Before 2010, the National Defence Concept of Estonia was founded on the principles of total defence and territorial defence. In 1993, the Parliament discussed the national defence concept prepared by the then Minister of Defence, Hain Rebane, but the draft act, 'Foundations of National Defence', was not approved. Even though a legal basis had not been established, the Defence Forces were built up according to the concept of total defence.

In 1996, the Parliament approved the first national defence concept, 'Main Directions of the Estonian National Defence Policy', based on the concepts of total defence and territorial defence. The document envisioned 'a joint and coordinated deployment defence, societal, and economic resources to prevent or divert threat or attack' (Riigikogu, 1996). The concept stated that in addition to military defence, the nation would develop Defence Forces with capabilities to provide military support to the civilian side to help to mitigate the consequences of natural emergencies, epidemics, and technical accidents, and to provide help to the civilian authorities in eliminating the consequences of disasters.

The National Security Concepts of 2001 and 2004 stipulated that the basis of the national defence was total defence that encompassed the whole of society. They required the state to ensure that all structures, including the Defence Forces and defence structures, had been prepared to avert threats, and stressed that national defence policy would be implemented by the application of total defence and territorial defence. The 2004 document and the Military Defence Strategy (2001) define total defence as the permanent psychological, physical, economic and other types of readiness of the state and municipal institutions, defence forces and the whole of society to manage crises; as well as coordinated and joint actions to prevent and divert assaults or threats and to ensure the survival of nation. All ministries and municipalities would participate in the preparation and execution of national defence that would comprise five components: military, civil, economic, psychological defence and civil readiness.

[8] By **Piret Pernik**, Research Fellow, ICDS (piret.pernik@icds.ee)

Later Military Defence Strategic Plan (2005) reiterated the principle of total defence.

In 2010, the new National Security Concept (NSC) was approved by the Parliament, and the National Defence Strategy (NDS), which replaced the previous Military Defence Strategic Plan, was endorsed by the Government. Both documents introduced a new approach: integrated national defence replaced the concepts of total defence and territorial defence. According to the NDS (MOD, 2010), the Military Defence Development Plan 2009-2018 was to be replaced by a comprehensive National Defence Development Plan (NDDP) 2013-2022. The Ministry of Defence (MOD) explained that in essence this meant that the national defence approach would be expanded from its previous strictly military domain to other domains (altogether six activity areas). This would require a joint development plan to be designed, since in the past national defence objectives had not been set for other domains.

III.2 Legal and institutional Framework

Estonia's current security and defence policies are based upon a broad concept of security and a broad-based approach to national defence, which have been formulated in the basic national defence documents: the National Security Concept (2010) and the National Defence Strategy (2010).[9]

The National Security Concept (NSC) defines the objectives, principles and priorities of the nation's security politics, and is one of the horizontal frameworks to be taken into account by all policy sectors when drafting development and action plans.[10] One of the key principles of the NSC is a broad approach to security, which considers all the factors influencing the nation's security. Its implementation encompasses all sectors vital to ensuring national security, including the following action areas:

- In the area of foreign policy, the implementation of a comprehensive approach, consisting of military and civilian instruments and development aid;
- In the area of defence policy, the implementation of a broad-based approach to national defence, consisting of military defence, civil contributions to military defence, assurance of internal security, international activity, securing the continuous operation of vital services, and psychological defence;

[9] The main legal acts regulating national defence are: the Constitution of the Republic of Estonia, the National Security Concept, the Peacetime National Defence Act, the War-Time National Defence Act, the State of Emergency Act, the Emergency Act, the International Military Cooperation Act, the National Defence Duties Act, the National Defence Strategy, and the National Defence Development Plan 2013–2022. According to the Peacetime National Defence Act, the basic plans for national defence are: the Bases of Security Policy, the National Defence Strategy, the Military Defence Development Plan, the Military Defence Action Plan, and the Emergency Defence Plan.

[10] The NSC is authorised by the Parliament following a proposal from the Government. The Government then approves the NDS and enacts the NDDP. Before authorising or amending the NSC, the Minister of Foreign Affairs and the Minister of Defence are required to consider the positions of the National Defence Committee and the Foreign Affairs Committee of the Parliament, and before authorising or enacting the NDS or the NDDP, the Minister of Defence is required to consider the position of the National Defence Committee.

- In the area of security policy, ensuring internal security as it pertains to national security, including protection of the constitutional order, resolution of emergencies, guarding the external border, and fighting terrorism, international organised crime, and corruption;
- Ensuring the resilience and cohesion of society, consisting of areas such as the continuous operation of vital services, electronic communication, cyber and energy security, transport infrastructure, security of the financial system and the environment, harmonised regional development, integration, psychological defence and public health protection (Riigikogu, 2010).

The broad-based approach to national defence encompasses all the options available to the state authorities and the population to ensure the nation's security in the case of military activity against Estonia. The comprehensive planning of national defence is based upon the **National Defence Strategy (NDS)**, which is based on the principle that all state authorities are responsible for their respective areas of competence both in peacetime and in the case of war; in other words, during all stages of the escalation of a conflict.[11] National defence planning involving all state authorities is based on the National Defence Development Plan (NDDP) 2013–2022, which specifies the courses of action and capability requirements of national defence.[12]

Since 1 January 2012, **the role of the Government Office in leading and coordinating integrated national defence has been strengthened** in order to better implement a broad-based approach. The National Security Coordination Unit of the Estonian Government Office was renamed **the National Security and Defence Coordination Unit of the Estonian Government Office** and two new positions were created to deal with issues relating to national defence. In addition to organising the operation of the Government National Security Committee, the Government Office was tasked with advising the Prime Minister on matters relating to national defence, and with coordinating the leadership of national security and national defence. The larger role given to the Government Office in organising national defence was motivated by a desire to improve cooperation between state authorities, streamline the decision-making process, and harmonise the main courses of action of national defence.

Separate ministries are in charge of the **six main courses of action of integrated defence**: the MOD is in charge of military defence and civilian sector support; the Ministry of the Interior (MOI) is in charge of ensuring internal security and sustainability of vital services; the Ministry of Foreign Affairs (MFA) is in charge of international efforts; and the Government Office is in charge of psychological defence.[13]

[11] During an emergency situation, the usual models of leadership and chains of command can change. The management of a state of emergency is led by the Government; with the Prime Minister in overall control.

[12] In January 2013, the Government enacted the NDDP 2013–2022, which specifies the courses of action and capability requirements for national defence. The plan, complemented by non-military action areas, will be presented to the Government in the 1st quarter of 2014. The NDDP replaced the earlier Military Defence Development Plan, which only dealt with military capability planning.

[13] The main laws governing the application of the broad-based approach to national defence are: in the area of military defence, the Peacetime National Defence Act, the War-Time National Defence Act, the International Military Cooperation Act, the Estonian Defence Forces Organisation Act, and the Defence

III.2.1 National Defence Act and NDDP

The National Defence Act is currently being drafted with the aim of implementing the principles of the NDS. It will amalgamate different national defence acts (the Peacetime National Defence Act, the Wartime National Defence Act, and the International Military Cooperation Act) into a single legal act.

The drafting of the **NDDP 2013-2022** started in February 2012, and before the end of the year it became clear that only the military part could be accomplished in time. By the end of 2013, the military plan had been complemented with the contributions of other actors. The main coordinator for drafting was the MOD, and the ministries participating in the drafting process were: the MOI, the Ministry of Communications and Economic Affairs (MEAC), the Ministry of Finance, the Ministry of Justice, the Ministry of Social Affairs (MSA), the MFA, and the Government Office. The Bank of Estonia and the Ministry of Agriculture have also been involved to a certain extent. A four year operation plan will be drafted once the NDDP has been approved by the Government, in the first quarter of 2014.

III.2.2 Institutional setup

Security and national defence issues are dealt with in three strategic-level meeting formats whose memberships occasionally overlap: the National Security Committee of the Government, the Crisis Committee of the Government, and the National Defence Council of the President. The key actors responsible for security and defence issues in the executive branch are the Government Office, the MOD, the MFA, and the MOI.

National Security Committee of the Government

National Security Committee of the Government coordinates the activities of the security services, assesses the national security situation, determines the need of the state for security-related information, and advises the government regarding the organisation of issues concerning national defence (including the submission of the NSC to the Parliament, the endorsement of the NDS and NDDP, preparations for mobilisation, the assignmet of national defence duties to government agencies, and decisions regarding additional resources for national defence.)

The committee is comprised of six ministers: the Prime Minister, and the Ministers of Defence, Foreign Affairs, Interior, Justice and Finance. To ensure more effective national security and defence governance at the government level, the Minister of Communication and Economic Affairs will also become a member of the committee.

League Act; in the area of civilian sector support, the Government of the Republic Act, the Law of Obligations Act, and the National Defence Duties Act; in the area of international efforts, the Foreign Relations Act; in the area of internal security, the Emergency Act, the State of Emergency Act, and special acts including the Police and Border Guard Act, and the Rescue Act; and in the area of continous operation of vital services, the Emergency Act.

Crisis Committee of the Government

Among other activities, the Crisis Committee of the Government monitors and analyses the organisation of national crisis management, including preparations for emergencies, the resolution of emergencies and the assurance of the continuous operation of vital services. If needed, the committee assists the authorities resolving an emergency with national impact or of particular severity in the organisation of the exchange of information and in co-ordination.

The committee is led by the Minister of the Interior and is comprised of the Permanent Secretaries of all ministries (except the Ministry of Culture, and the Ministry of Science and Education). Members of the committee include also the Secretary of State, the Director General of the Rescue Board, the Chief of Staff of the Headquarters of the Defence Forces, the advisor to the Prime Minister for national defence issues, and other senior government officials.

National Defence Council

The National Defence Council of the President discusses issues important to national defence and gives its opinion on them. Members of the Council are the Prime Minister; the Ministers of Defence, Foreign Affairs, Finance, Interior, and Justice; the Speaker of the Parliament; the Chair of the National Defence Committee and the Chair of the Foreign Affairs Committee of the Parliament; and the Commander of the Defence Forces. It is planned that the Minister of Communications and Economic Affairs will also become a member of the Council.

Government Office

The Government Office assumed a greater role in national security and defence issues less than two years ago. The reinforced Security and National Defence Coordination Unit, which coordinates security and national defence issues, is responsible for only one activity area of the NDS: psychological defence. The **Office has no decision-making authority over the ministries, and no legal mandate to enforce the implementation of government decisions.** In Estonia's governance system, the ministries themselves are responsible for the implementation of government decisions that concern their administrative areas, but in doing so they tend to neglect the wider, whole-of government approach.

There is little that the Government Office can do to improve ministerial performance beyond providing counsel. Rather, its **role has been to work to balance the interests of different ministries and seek common ground**. As noted previously, its legal mandate includes advising the Prime Minister on security and national defence issues, managing the operations of the Government's National Security Committee, and coordinating the command of security and national defence. The recent steps to grant a greater security and national defence role to the Government Office are welcome in this background.

In addition to the reinforcement of the Security and National Defence Coordination Unit, a position of the **National Defence Adviser** of the Prime Minister (presently a retired general) who supports him on security and defence issues has been established. Moreover, a government official disclosed that in

the near future the Government Office will assume the lead coordinating role in drafting the fundamental national security and defence documents such as the NSC (drafting this document has so far been the responsibility of the MFA) and NDS (so far the responsibility of the MOD).

Ministry of Defence

The MOD formulates national defence policy and participates in the formulation of national security policy. It also coordinates the implementation of NDS and the development of NDDP. The subordinate agencies executing these policies are: Defence Forces and Defence League, Defence Resources Board, Information Board (external intelligence service).

Ministry of the Interior

The MOI has the missions of assuring the internal security of the state and protecting public order, guarding and protecting the state border, and assuring the border regime. The MOI is also tasked to regulate crisis management and rescue works. It develops internal security policies and plans, including for wartime. The subordinate agencies executing these functions and policies are: Police and Border Guard Board, Rescue Board, Internal Security Service (Kapo).

Ministry of Foreign Affairs

The MFA formulates and implements main directions of foreign policy, and organises and coordinates international relations of the republic. It works out the draft security policy concept in cooperation with the relevant government agencies. In wartime and under the conditions of mobilisation it prepares and organises diplomatic representation with foreign states and international organisations.

Ministry of Economic Affairs and Communications

The MEAC organises the continuous operation of the 19 vital services including electricity, fuel and gas supply; transportation (airports, ports and railway) and roads; communications and broadcasting networks; uninterrupted communication, etc. Its tasks in preparation for wartime include determining the wartime needs of the industrial sector and preparing the wartime tasks assigned to the industrial sector, as well as organising the acquisition and storage of the relevant stockpile. It prepares the organisation of construction and public work corresponding to wartime condition. It works out building regulations and operational rules for railways, waterways, roads, ports and airports, as well as prepares the organisation of transport operations and traffic corresponding to national defence requirements.

Ministry of Social Affairs

The MSA organises the functioning of in-patient specialised medical care and emergency medical care. It also organises functioning of drinking water safety control and blood service. Under the conditions of mobilisation and wartime the MSA prepares and organises the provision of medical care and the prevention of outbreak and spread of infectious diseases.

Ministry of Agriculture

The Ministry of Agriculture organises the continuous operation of the functioning of the control of food safety. The Ministry of Agriculture or an authority within the area of its governance forms the state food stockpile for wartime.

Other ministries

In addition, the Ministry of Environment, the Ministry of Justice and the Ministry of Finance are in charge of organising sustainability of vital services of special importance for security and integrated defence under their respective areas of governance. The Ministry of Culture and the Ministry of Education and Research contribute to integrated security and defence in the area of psychological defence.

Organisation at the regional level

There are four permanent regional crisis committees, established by the Minister of Interior, tasked with coordinating crisis management within its geographical area of responsibility. Each regional crisis committee is headed by the Director of the Regional Rescue Centre and includes representatives from the Police and Border Guard (the prefect, also acting as deputy chairman), the governors of each of the 2-6 counties situated in the region, the mayors of the cities situated in the region, representatives from the Defence Forces, the Defence League, the Internal Security Service, the Environmental Board, the Environmental Inspectorate, the Estonian Road Administration, the Health Board and the Veterinary and Food Board. The regional crisis committees, based on the Emergency Act, have currently no role in case of an armed attack on Estonia as this Act does not regulate preparing for and resolving an emergency arising from a military threat.

The regional level reflects the lack of coordination in organizing the work of Governmental authorities. The geographical areas of responsibilities of Regional Rescue Centres (*päästekeskus*) and the Police and Border Guard correspond, but they differ from the regional organisation of the Health Board, the Environmental Board, the Emergency Calls Centre (*häirekeskus*), the Emergency Medical Service (*kiirabi*) and the Defence League.

The Defence League was, in 2013, tasked to organise territorial defence, but there is no regional command level. Instead, it is current territorial structure is based on the pre-Second World War districts that do not correspond fully with the current 15 counties of Estonia, nor with the boundaries of the four regional crisis committees. An important function in any nation is Emergency Medical Service, and, starting from 2014, this service is organised in ten geographical areas that do not correspond with any of the above mentioned organisations.

Crisis escalation stages

Crisis regulation is stipulated in the Emergency Act, which covers the preparation for an emergency, the response to an emergency and the continous operation of vital services.[14] It also provides the procedures for the declaration

[14] According to the Emergency Act, crisis management is a system of measures which includes

of an emergency situation and sets out the coordination necessary to resolve an emergency situation. In addition two other types of situations that may threaten national security are described in the national legal framework: a state of emergency caused by a threat to the constitutional order; and wartime (Riigikogu, 1996/2011; Riigikogu, 1994/2012).

In the case of an emergency, the leadership structures, the authorities of the institutions, and the responsibilities of the actors will not alter from their day-to-day functions and operations. However, in the case of an emergency situation the usual models of leadership and chains of command can change. Similarly, during the management of a state of emergency that is led by the Government, the Parliament may authorise the head of a state of emergency (the Prime Minister) to apply methods applicable to a state of emergency that may differ from daily operations. During wartime, the leadership structures may also alter. For example, the Commander of the Defence Forces may command and order individuals and legal persons who are not under his authority to execute duties related to national security that they have been assigned (Riigikogu, 1994/2012).

III.2.3 Best practices in inter-agency interactions

In some narrower areas of national defence and crisis management, inter-agency interaction has been well established. One positive example of inter-agency interaction is the process of the **risk analysis of emergency situations**. This biennial process ensures that all involved parties have a common understanding of internal and external civil protection risks, and that methods to prevent, respond to and mitigate them will be planned and resources will be allocated. This process is led by the MOI, and all public and private sector actors in the area of civil protection are engaged (ministries and their subordinate agencies, critical infrastructure owners, etc.). The risk analysis describes emergencies, the threats that cause them, the likelihood that emergencies will take place, and their consequences. The government agency that, according to the Emergency Act, is responsible for contingency plans in its area of responsibility earmarks the resources required for managing crisis within this area (e.g. the MFA will draw up a contingency plan for consular incidents that may affect Estonian citizens abroad, and will earmark the resources needed to resolve them).

Another successful example of inter-agency cooperation that has been operational for many years comes from the area of **civilian support to the military: the reception of allied military forces.** Experts interviewed fro this report agreed that the provision of civilian support to the military is well organised and that the interoperability of different actors is well developed. The legal framework for Host Nation Support sets out clear mandates, responsibilities, and tasks for all actors, and practical cooperation is regularly trained. Likewise, **military support to civilian emergencies** is also well organised. The Defence Forces have made their **resource catalogues available to the civilian authorities**, and military officers participate in regional crisis committees, alongside police and rescue services officers.

---

preventing an emergency, preparing for an emergency, resolving an emergency and mitigating the consequences of an emergency (Riigikogu, 2009).

The annual Host Nation Support exercise, 'Baltic Host', provides a practical testing ground for host nation inter-agency interaction. In November 2013, the exercise took place in conjunction with the NATO Response Force exercise, 'Steadfast Jazz'. In addition to the Defence Forces, the Government Office, the MSA, the MEAC, the Defence Resources Board, the Police and Border Guard Board, the Rescue Board, the Estonian Maritime Administration, the Estonian Road Administration, the Estonian Health Board, the Estonian Technical Surveillance Authority, and the Estonian Internal Security Service took part in this exercise. Several state-owned and private sector enterprises also participated (e.g. the electricity system operator Elering, Estonian Railways, the Port of Tallinn, and Tallinn Airport).

Another positive example of the implementation of the concept of integrated defence is provided by the **Defence League**. Members of the League represent many civilian professions in the public and private sectors (policemen, firemen, rescue workers, doctors, IT-specialists, etc.). These people will use their personal and professional links and networks to fulfill their national defence tasks within the League. Another excellent example of public-private partnership is the **Cyber Defence Unit of the Defence League**, where voluntary contribution is seen as a force multiplier – voluntary members are willing to contribute even more than hired IT-specialists.

III.3 Expert opinions

This part of the report gives an overview of the opinions of 18 government officials, who were interviewed about the success of the implementation of the concept of integrated national defence.[15] It is structured according to the key factors identified by the officials to have had the greatest impact on implementation: philosophical understanding of integrated (broad based) national defence, strategic and long-term planning, and coordinated implementation.

III.3.1 Philosophical understanding of integrated national defence

The majority of experts said that the implementation of the integrated national defence system would take many years, because it **requires the altering of old mindsets, traditions and habits, the introduction of new planning procedures, the solicitation of common understandings**, etc. Some of the experts argued that the understanding of current security trends at the political level and in society is inadequate -- commercial and soft values predominate over hard security concerns, although the latter have not disappeared. It was argued by one expert that many politicians and high-level government officials who are not dealing with national defence issues do not understand why the state should spend on defence, especially as allied and national threat perceptions rule out the possibility of military conflict in the scope of the next decade. However, as the security context changes, the NSC and NDS – the state's

[15] Interviewed experts were currently employed, or had been employed in the recent past in: the Defence Forces, the MOD, the MOI, the MEAC, the MSA, the MFA, the Government Office, the Police and Border Guard Board, and the Rescue Board. They included officials in strategic leadership (Permanent Secretaries, Undesecretaries, Deputies to the Heads of the Institutions), Heads of Departments, and working level experts.

fundamental security and defence documents -- should be reviewed periodically, and more often than currently, because the global and regional security situation changes much faster.

Many experts agreed that **Estonian society needs a broader, academic discussion** about the long-term strategic security and defence vision**. A contract between the major political parties** that set priorities and allocated resources to address the regional aspects of national security would be welcome (e.g. the parties could agree to maintain a symbolic presence of the Defence Forces in Northeast Estonia). The gulf in mindsets and perceptions between the Government and Parliament on the one side, and society on the other side, is deep; as as is the divide between bigger towns and peripheral rural areas. The Government should thus initiate a broad-based discussion involving universities, think tanks, parliament, opinion leaders, etc. on the purpose and vision of integrated national defence.

The concept of integrated national defence is also understood very differently among government actors – each actor interprets it in a way that is convenient for them. **Integrated national defence has not been implemented in the strategic planning processes.** The Government has not formed a common view on national defence issues, individual ministers compete with each other for resources, and **each ministry approaches national defence issues from its own vertical silo**. In the Estonian governance model, **each ministry has full authority over its policy domain**, and as the Prime Minister commands no authority over the ministers, he has no instrument to enforce Government decisions against will of a minister. Each ministry has full independence over its administrative area and there is no overarching authority or strategy that would harmonise their activities.[16]

The experts reiterated that **in essence, integrated national defence is nothing new: it is total defence**. Total defence and integrated defence can both understood as the mobilisation of the resources of the whole of society to defend the state during periods of crisis and war. The concept of **'integrated national defence' extends the domains of activity of total defence by adding international activity, and ensuring internal security and the provision of vital services**. Thus, integrated national defence encompasses, in addition to military defence and civilian contribution to it, many non-military areas. In a worse-case scenario, an adversary will make use several of these domains and may exploit many tools in a coordinated manner. This means that the state must prepare to defend against military and non-military threats. The NDS asserts that in the preparation for crisis and in times of crisis, state, actions must be coordinated at the operational level taking into account a whole-of-government perspective. The strategy provides a framework for 'pooling and sharing' – i.e. allowing military and civilian assets to be used interchangeably.

Both fundamental security and defence documents – the **NSC and NDS** – **received some criticism** from the experts. One expert claimed that the NSC is not

[16] Estonia's governance structure is founded on a system of independent ministries, each responsible for its own area of competence. The Prime Minister's role is one among equals. *OECD Public Governance Reviews: Estonia.* (OECD 2011:120).

a systematic document, because national interests have not been prioritised and categorised, and methods to achieve them have not been designated.[17]

Likewise, the NDS should be viewed as a political statement rather than as a strategic guideline, and it does not fulfill the criteria for a national strategy -- the means to achieve the ends, and where these resources should come from have not been designated. It is thus **difficult to make strategic plans based on these documents**. Another expert believed that the NDS is an entirely unprofessional and abortive document. He claimed that as a planning document it is obsolete, because the authorities and mandates of different government institutions overlap in all six activity areas, and it is not clear what a particular area consists of and who is responsible for activities within it (e.g. civil support to military defence; international activities, securing vital services).[18] He also suggested that the government's endeavour to develop the NDDP 2013-2022 through inter-agency process was not sensible, because the task was overwhelming.

Interestingly, even though all experts believed that the underlying principles of the NDS have been understood and accepted by all actors, some experts claimed that the principles have been discussed and argued over only in a small circle of government officials. A few experts thought that some of the principles may be imprudent in practice, and should be reconsidered through broader and academic discussions. For example, the principle that all actors will be responsible for the same activity areas across all crisis escalation levels was questioned – it was argued that in the case of mobilisation much more authority and greater capabilities would be needed, and thus responsibilities should shift.[19] Another expert suggested that the concept of integrated defence is not completely clear, and that **a lot of discussions, engagement, practical workshops and exercises would be necessary to reach a common understanding and mindset**.[20]

It was also argued that although everyone understands and supports the principles and objectives of the concept of integrated national defence on a general level, **there is lack of understanding of the essence and implications of the concept across all ministries,** resulting in a lack of competence. This, in turn, hinders the implementation of the concept. The ministries organise their

[17] At the same time, one respondent argued that the Parliament should approve only some general philosophical guidelines of national security, and not an executive document that determines the objectives, actions, means and resources for attaining national interests.

[18] By contrast, the previous version of the document, the military strategy from 2001, clearly laid out who is responsible for what (e.g. the MSA prepares for and executes healthcare services during crisis and war times), and what each activity area consists of (e.g. civil readiness included the preparation for crisis and war time; as well as all activities for ensuring the long term functionality of the defence forces and society during crisis and war time).

[19] Mobilisation means the transfer from peacetime to wartime readiness and, in addition to the military, it includes other actors: police and internal security forces, rescue services and border guard, military and civilian healthcare system, etc. During crisis or war there will be additional demand for law enforcement to support military activities (e.g. the police will organise the evacuation of citizens, there will be greater demand for medical services, etc).

[20] The same lack of clarity also affects other cross-sectoral policy subjects (e.g. for many years the Ministry of Finance has coordinated inter-agency strategic planning and personnel policy; nevertheless, there is still no clear conceptual understanding by government actors of how to manage these subjects, what is the subject matter to be coordinated, etc.).

activities for peacetime duties only, and **it is erroneously believed the MOD is responsible for wartime preparations**. As one expert put it:

> Prior to the amendment of the Constitution in 2011, Estonian officers did not understand why the proposed changes were needed. Even today there is a lack of understanding across the ministries in respect to their distinctive roles in implementing integrated defence; there is a mistaken but widespread view that national defence issues ought to be handled and financed by the Ministry of Defence.

Another expert suggested a way forward:

> We need to create an understanding that the peacetime and wartime structures and composition of the defence and internal security forces are different. We need respective contingency plans that take into account which additional resources are needed across all NDS areas. We need to determine the responsibilities and obligations of state institutions, municipalities, private companies, and individuals during crisis and wartime; each party has their own role in national defence.

Thus, while it was confirmed during the interviews that, in general, **actors do understand that the roles and responsibilities of different actors will remain the same during different crisis escalation levels**, there seems to be **at least some degree of confusion regarding who does what** that merits more detailed explanation. For example, the leadership of the Rescue Board stated that the Board would continue its peacetime activities during wartime, that it would prioritise its activities according to the needs of national security (e.g. some peacetime services would not be provided), and that wartime activities would be carried out under different (military) command. However, according to one interviewed expert, the leadership of the Board has no clear understanding of the kind of command structure under which it would operate during a state of emergency or in wartime.

The interviews also revealed some **distrust between the actors that suggests a lack of information or insufficient interaction**. One respondent believed that MOD exploits the concept of integrated national defence as an opportunity to delegate to other actors the military defence-related duties that it is ought to take care of itself. It was also believed that only a small circle of officials who deal with the issue on a daily basis really understand it, while the leadership of the ministries does not perceive the necessity to implement the concept in practice (mainly because security risks and threats addressed by the NDS are not imminent). It was also suggested than an outside objective expert view would be needed.

With regard to the civilian health care sector, interviewees argued that **the concept of integrated defence has been accepted by all actors, but that this has not been enough to implement it in practice**. They suggested that, most importantly, the MOD and Defence Forces ought to explain to the health care sector its concrete roles, responsibilities and duties, and identify indispensable capabilities for performing these roles; the health care sector itelf does not have the competence and resources to do so. Likewise, with regard to developing the military health care system for wartime, the MOD and Defence Forces ought to have at least a basic knowledge of the civilian health care system (which they currently do not), and the separate systems should be developed in coordination

(which they have not been) to ensure that they will be interoperable (which at the moment cannot be guaranteed). Thus, mutual education on the military and civilian health care systems should be provided for both civilian and military actors, and the development plans of those systems should be coordinated..

III.3.2 Strategic, mid- and long-term planning

Estonia's public administration functions on the basis of **multiple strategic plans, many of which are not implemented**.[21] The majority of experts stressed that the establishment of strategic and long-term planning will take many years. It has taken ten years for the MOI to build up a crisis management system and the key requirement to apply whole-of-government approach to crisis management -- that ministries fulfil their functions effectively – has still not been attained. **Strategic planning capabilities are weak in all ministries across all policy areas.** Another obstacle for whole-of-government strategic planning is the **lack of a central coordination authority to guide and oversee the process**. Presently, each ministry develops its own development plans, which may not relate to each other. Horizontal coordination across cross-sectoral policy subjects should be strengthened, and the central coordinator must gain legal mandate to oversee and -- if necessary -- to coerce other ministries to implement decisions of the government.[22]

There is great difference between the **well-established strategic planning system within the military (and to a lesser extent in the law enforcement agencies)** that has been practised since the preparation of the first Annual National Programme in the framework of the Membership Action Plan at the beginning of the millennium, and procedures in other government agencies which have no such experience. NATO's strategic planning manual, used by the Defence Forces, is too complicated to suit other actors. An associated challenge is the **need to change the mindsets of other actors so as to be receptive to long-term strategic planning**. A further obstacle is the **unpredictability of financial resources in the mid- and long-term for all ministries other than the MOD** (there is political consensus to allocate 2% of GDP for defence spending in long-term). The organisational development plans of other ministries are linked to the state budget strategy and take only a four-year perspective. Their annual budgets are thus subject to greater flux, and within these budgets the proportion that is to be spent on security and defence capabilities is not specified. Struggling with shrinking budgets and incremental increasing expenditure, the **ministries tend to spend all their money on current functions, and not on preparation for possible security threats in the distant future**. One expert suggested that variations in the annual budget of the Ministry of Defence affect merely the amounts available for investments, while for other ministries the fluctuation of budget also impacts everyday functions, not to mention planning.

[21] Currently there are three key horizontal documents in place providing the main strategic direction, among them the NSC. OECD Public Governance Reviews: Estonia.(OECD 2011:173).

[22] The Government Act establishes a decentralised governance model with each ministry having full independence over policy making within its administrative area. The Act does not provide for a horizontal cross-sectoral coordination role for a single ministry, and this causes a fundamental problem for horizontal cooperation in all areas where cross-sectoral coordination is needed (internal security, vital services, etc.).

Most experts agreed that their ministries and subordinate agencies should plan and prepare for their wartime national defence duties and tasks, but they do not know how to do that. They look to the MOD to provide guidance. Furthermore, the leadership of the ministries have no information about how the other ministries are planning to organise their activities within the framework of the NDDP. The actual implementation process of the NDDP, which will start in 2014, will show if different ministerial development plans are compatible and if national defence capabilities are interoperable.

The development of strategic planning is also constrained by a lack of expert opinions on the criteria against which to evaluate wartime civilian capabilities. For example: who should set the requirements and standards for the functioning of mobile communications during the full spectrum of emergency situations and in wartime; or who should set the traffic volume requirements for roads and bridges? The Defence Forces and the ministries who are responsible for these policy areas have **no expertise or resources to hire additional staff members to solve the issues that fall between the administrative areas of individual ministries**.

Another complication is the **abundance of strategic and development plans that have not been coordinated with each other**. In addition to cross-cutting sector-wide governmental development plans (*valitsuse arengukavad*) each ministry has its own mid-term organisational strategies, which have not usually been coordinated with each other. Often, they do not take into account overarching horizontal security documents such as the NSC, or other cross-sectoral strategies such as the NDS.

Inter-agency cooperation is well established at the operational level (see the 'coordinated implementation' section of this chapter below); however, this is mainly due to personal relations. Achieving joint strategic planning across the ministries has been more difficult and here, each ministry strongly prioritises its own policy areas.

Sometimes, **ministerial development plans will be drafted or projects initiated without coordinating with the actors who will be involved in their implementation**. One interviewee alleged, for example, that no representative of the civilian healthcare system participates in the development of the annual military healthcare plan; or vice versa, the civilian good will agreement on healthcare has been developed without the participation of a military officer. Another example was brought by the MOD: **ministries tend to coordinate their projects too late and as a result, national defence requirements are not met**. Another problem pertaining to resources is that when national defence requirements require additional investments, it is not clear who should cover them: the ministry who owns the project or the MOD.

III.3.3 Strategic planning manuals and toolboxes

In general, all interviewees supported the idea of introducing **specific strategic planning manuals and toolboxes**. A practical and concise **manual** (as phrased by one respondent, a 'doctrine') to raise awareness on the political level and amongst the population at large would be useful. Another expert believed

that **an inter-agency handbook for planning**, describing what was to be done and who would be responsible, would be important.

However, it was also suggested that **abstract educational tools are not needed** at the working level, for government officials whose everyday duties include planning for integrated national defence. First, the only officials able to write the manuals would be the same handful of experts who actually need to implement the integrated approach; second, at the working level, there is already consensus on objectives and methods - the issue is rather how to overcome structural problems.

One expert insisted that the problem lies not in a lack of guidelines or tools, but in a **lack of competent personnel with in-depth expert knowledge on particular narrow policy subjects**. So far integrated national defence planning has remained on a very general level due to a lack of competent experts able to assess the impact of the different factors and events described in the threat scenarios. For example, in the case of a particular internal/domestic security incident, assessments are required of which vital services would be continuously provided to the population, to what extent and in which regions, what the effects of disruptions would be, which capabilities and equipment would be needed, etc. Currently there is a lack of such experts behind the planning tables.

It was also maintained that for a small nation such as Estonia, the best strategic planning tool would be a **practical and concise description of the working procedures (Standard Operating Procedures).** The aim of such a practical regulation (*eeskiri*) that can be applied at the operational level during exercises is to facilitate practical inter-agency cooperation.

III.3.3 Financial and human resources

In most ministries other than the MOD, **financial resources are planned only for day-to-day activities**. One respondent estimated that due to cuts and frugality, **in some areas of civilian crisis management even the most basic capabilities are missing**. Police, rescue service and health care sector experts argued that the annual budgets of their agencies are not sufficient for even their day-to-day activities making it doubtful that additional resources could be allocated. Moreover, preparation for wartime tasks has not been an immediate concern for ministers, and there is an overall lack of resources for investments and for the development of wartime capacities. **Capabilities for major emergency situations can be assembled, and ministries have prepared for non-military emergency scenarios, but scenarios and preparations should also be extended to wartime**. Current levels of readiness are insufficient for the larger scale capabilities needed in wartime. Medical reserves (*tegevusvarud*) are planned for emergencies, but do not take wartime needs into account.

In some policy areas a solution could be the **more efficient cross-sectoral use of existing capabilities and assets**. For instance, instead of providing a civilian general practitioner (*perearst*) to active-duty military personnel (*tegevväelane*) and to conscripts, a contingent doctor could fulfil this role; similarly for nurses and other medical personnel in support functions. Streamlining would help to save money that could be used for wartime preparations. One positive example is that the MOD supports the teaching of

war and disaster medicine in higher education medical schools and universities for nurses, midwifes, and doctors (for doctors it is mandatory).

III.3.4 Coordinated implementation

A prerequisite for the voluntary engagement in and commitment by all actors to the implementation of the NDS is the achievement of consensus about the substance of the concept. This will take many more years of concerted effort, as explained in previous sections of this chapter.

Still, most experts agreed that **working level inter-agency interaction functions fairly well**, although it still needs to become more effective and efficient, and resources should be better planned. As put by a senior expert: 'in military terminology **we have achieved clear "unity of purpose", and now we need to achieve "unity of effort"'**.

Integrated national defence involves a large number of ministries, and the engagement of ministries who are inexperienced in the culture of strategic planning is a huge challenge. Better coordination mechanisms will be needed for the successful implementation of the concept. Because ministries are driven by narrow mandates, **an overarching central authority** should be established to form a whole-of-the-government picture of national defence. **There should be a clear procedure for taking contentious issues (e.g. issues concerning resources that ministers cannot agree on) to the Government level**. So far, such issues have been discussed only at ministerial level (and solutions have not been found).

In some policy areas, for example in the area of civilian and military healthcare, **a joint 'owner'** would be necessary. As discussed in the 'strategic planning' section of this chapter, these two systems are planned by different actors (the MSA and the MOD), and more coordination is needed to ensure their linkage.[23]

While in principle all actors support the objectives of integrated national defence, the devil lies in the details. Ministries are reluctant to entrustassets to other actors or delegate some of their own authority. The **leadership of the ministries expects stronger guidance from the MOD regarding how they should prepare wartime capabilities and assets** (including detailed information on numbers of items, their characteristics, etc.). At the same time, respondents believe that the MOD expects other ministries to provide ready-made lists of all their capabilities and assets, from which the military could choose those appropriate to their own needs. These different expectations constitute an obstacle to working level implementation.

It was proposed that the **undersecretaries of the ministries should meet regularly to discuss national security and defence issues**, and that these meetings could provide inputs into the formulation of the agenda of the meetings of the Government's National Security Committee. It has not so far been determined which meeting (e.g. the National Security Committee, the weekly meetings of the Prime Minister, the Minister of Foreign Affairs and the

[23] The MSA and the Health Board do not have the resources to create a coordinated position. The MOD has developed capabilities for strategic planning: they should consider taking a greater role in coordination.

Minister of Defence, the entire Government) should address which issues, and it was feared that this would lead to a situation in which the opinions of some actors would be disregarded. It was suggested that **clear guidance should be issued to the ministries on the type of questions (international missions, procurement, etc.) to be addressed in the various meeting formats.**

III.3.5 Central coordinating authority

Interviewees believed that the MOD, which was assigned an inter-agency coordinating role by the government for the NDS, and which in 2012 coordinated the failed effort at inter-agency process for the whole-of-government NDDP, was not capable of engaging other actors. They suggested that the endeavour failed because the MOD failed to explain the need for the development plan to other actors, did not acknowledge the scope of the challenge, and did not have the necessary experience and competence for the task.

The majority of experts admitted that **the coordination of cross-cutting issues is currently inadequate**. Each ministry that is in charge of one activity area of the NDS should invite other actors to issue-based working groups or seminars, and explain procedures, roles, and coordination mechanisms. **Regular and practical inter-agency training and exercises would also be most useful.**

As regards the coordination of the provision of vital services, respondents suggested that centrally organised coordination by one ministry would be more efficient than the promotion of horizontal communication between sub-units across different administrative areas. According to the Emergency Act, the continuous operation of vital services shoud be organised by the ministry that owns the administrative area to which a provider of a vital service belongs. For instance, the MEAC should organise the continuous operation of the functioning of the electricity supply.[24] The ministries co-ordinate the assurance of the continuous operation of vital services within their administrative areas, and advise supervise the providers. The MOI is assigned a central coordinating role as it coordinates the organisation of the continuous operation of vital services with the ministries and other state authorities, but not directly with the providers of vital services.[25] One expert suggested that a central coordinating organisation (the MOI) should coordinate with all providers of vital services, including determining their required capabilities, identifying risks and threats to critical infrastructure, and sharing this information with other relevant government and private sector actors. For example, the Cyber Defence Unit of the Defence League does not have sufficient personnel to carry out coordination with more than 200 providers of vital services.[26]

[24] The continuous operation of a vital service is the capability of the organiser of the vital service to function consistently and the ability to restore consistent functioning after an interruption (Riigikogu, 2009).

[25] A provider of a vital service is a state or local government authority or a legal person whose competence includes the fulfilment of a public administration duty defined as a vital service in section 34 of this Act or a person operating as an entrepreneur providing a vital service in the case specified in subsection (2) of this section (Riigikogu, 2009).

[26] In the organisation of mobilisation it was suggested by an expert from the MOD that the MOI, and not the MOD, should coordinate with local municipalities.

Respondees argued that the coordination of national defence with local governments could also be carried out more efficiently by a central coordinating body. The MOD requested the MOI to coordinate with local governments to ensure that, during mobilisation, local governments would have enough personnel to execute the duties assigned to them by the Peacetime National Defence Act. A national defence expert noted that the MOI, which is responsible for wartime internal national security plans and so should also have taken care of the organisation of local government duties during mobilisation, declined a coordinating role.[27] This indicates that the understanding of the roles and duties of different ministries in national defence is not uniform, posing difficulties for interaction.

Most experts agreed that the **coordination capabilities of the Government Office should be reinforced, and that the Government Office should assume a more proactive approach.** The Government Office should also assume a stronger role in inter-agency coordination by advising the Prime Minister on national defence issues in a timely manner, and by bringing issues to the Cabinet, or to the National Security committee of the Government (it was felt that the Government Office has so far been modest in doing so). It was strongly recommended that the Government Office should also take a much more proactive approach in managing the meetings of the Security Committee of the Government, including in forming its agenda, formalising meetings and agenda-setting, following-up on decisions, preparing substantial minutes, etc.

Experts also supported a proposal that **the mandate of the National Security Committee of the Government should be expanded**, and that its legal framework should be reviewed and amended. It was also suggested that the Security and National Defence Coordination Unit should be staffed by politically unaffiliated policy experts (advisers on military, healthcare, crisis management and other security and defence issues) to facilitate the flow of expertise from the working level to the National Security Committee of the Government, and to the Government at large, and to create a whole-of-government view on each issue area. One senior expert suggested that the **Headquarters of the Defence League could advise the Unit on the organisation of a whole-of-government command and strategic planning system**.

The large majority of interviewed government officials maintained that the legal mandate and decision-making authority of the Government Office should be strengthened. It was believed that no one opposes this proposal in principle, but when it comes to practice, the **ministries are unwilling to give up their existing authorities or responsibilities**. At the same time, one government official underlined that while the Government Office should assume a stronger coordination role, **authority for command should remain in the ministries responsible for a particular national defence issue** (e.g. in the areas of crisis management the MOI). According to one expert, the central governance

[27] According to the Peacetime National Defence Act (Riigikogu, 2002/2013), mobilisation means the bringing of the defence forces, national economy and state institutions from a state of peace to a state of war. The MOI works out national internal security plans for wartime and performs other tasks assigned to it by Acts for guaranteeing internal security. Local government facilitates, within its territory, the evacuation of persons, the accommodation and supply of the evacuated and the provision of medical care to them.

authority (whether the Government Office or some other body) must make sure that the ministries actually implement the decisions of the Government and its National Security Committee and that this must be done from a whole-of-the-government perspective, and not according to stove-piped interests and priorities.

Several experts saw a need for a central authority with a legal mandate to direct other ministries. It was frequently stressed that the fact that, in Estonia's governance model, the ministry responsible for a particular policy subject has no legal mandate to force other ministries to meet their obligations constitutes a national security problem (e.g. the Ministry of Environment was obliged to prepare 24/7 radiation protection capabilities, but has not done so, while the MOI, which is responsible for internal security and crisis management, can do little more than point out the existing deficiencies in radiation protection capabilities).

III.3.6 Leadership and command structure for integrated defence

The issue of leadership and command structure was the biggest mystery for the interviewed government experts. While all experts agreed that the ministries would continue to implement their peacetime tasks during non-military emergencies and during military conflict or war, there was significant confusion and a lack of knowledge about authority, and the leadership and command structures. The experts pointed out that the **legislation does not describe how the transfer from peacetime to wartime will be conducted** -- who is responsible for what; who does what? Likewise, it **has not been determined how mobilisation will be organised**. Fortunately, this confusion will be solved in the near future as the Government plans to draw up an **operational command plan for strategic-level government leadership**.

Institutions whose day-to-day business involves national defence tasks, expressed the view that every ministerial administrative area would retain command over its activities during all stages of escalation, and that the Government Office would oversee the cross-border command structure. In institutions that do not handle national defence issues on daily basis, there was an expectation that in the case of a serious internal or external security threat, a commander of the emergency would take command of the activities of their agencies, but it was not clear what the new command structure would look like at the strategic and operational political and military levels.

All in all, leadership and command structure posed the biggest question mark for the experts. **Some leaders of ministries and their subordinate agencies admitted that they did not know who would command them during some escalation situations** (state of emergency, wartime). For example, one expert said that the leadership of the Rescue Board has no guidelines for a state of emergency or wartime -- they do not know what they should be preparing for, where the resources should come from, who will command them and under which mandate, or what their strategic mission, priorities, and tasks should be. Hence, arguably, they are currently unprepared for the wartime duties assigned to them by legislation, such as assisting in the evacuation of civilians.[28]

[28] According to the NDS (MOD, 2010), the police and rescue services must assist in the evacuation

Many experts pointed out the principle prescribed by the Emergency Act and the NDS, that the institution under whom responsibility for a particular crisis falls would lead the management of this crisis both during peacetime and wartime. For example, the Estonian Internal Security Service would lead on the management of a crisis caused by terrorist attacks and cybercrime. However, given that a terrorist or cyber attack may result in a technical disaster or accompany a national security threat, it is not explicit which actor should take overall command. **National security threats are likely to involve multiple dimensions (internal and external security aspects, cyberspace, etc.) that may cause confusion with regards to the identity of the overarching leadership.**

It was also understood that during peacetime the Defence League supports the police and rescue services, but prior to escalation into military conflict the Defence League would be supported by them. However, it has not been considered when and how this would happen on the strategic and operational levels.[29]

In addition to the need to explain the nature of the command structure at different escalation stages to the leadership of government institutions, it is necessary to ensure that in the case of a crisis, the command structure can be assembled quickly and make effective decisions. One expert proposed that procedures and practical regulations (Standard Operating Procedures) should be put in place for doing so. Another crucial aspect is the need to ensure a bottom-up flow of information to enable effective decision-making. One expert suggested that the procedures of the relevant government agencies (the police, the Internal Security Service and others) for informing the state's strategic leadership in the case of crisis should be specified and described in legal acts, as no regulations exist at present.

The experts had different opinions regarding the need of aligning geographical division of services of various agencies, in order to ensure their effective coordination and collaboration during crisis or in wartime. For example, a representative of the MOI deemed the fact that geographical areas of service of the Emergency Medical Service differ from the four regions of Police and Border Guard Board and Regional Rescue Centres poses a problem for crisis management activities. At the same time, a representative of the Health Board regarded that the current geographical areas of the Emergency Medical Service are optimal and allow providing the highest quality of medical service to the population. He believed that if they were completely aligned with those of other agencies (e.g. Regional Rescue Centres and Police and Border Guard Board), the Emergency Medical Service's ability to deliver its services at the required level of quality would be impaired.

III.3.7 Legal framework for integrated defence

The NDS should be embedded in specific laws and regulations (e.g. the Government Act), and the statues of the ministries should be amended to include the responsibilities and duties stemming from the strategy.

---

of the civilian population.

[29] The Defence League has formulated a draft doctrine that will address some of these issues.

National Defence Act

One government official suggested that it will not be enough to address only the strategic command structure and planning, but that the new Act should incorporate a broader view encompassing all six activity areas of the NDS within a single framework. The view that the National Defence Act should determine clear and logical responsibilities and obligations for all ministries and government agencies, while lesser legal means (e.g. Government decrees) should describe in greater detail the command structures and processes of crisis regulation during non-military emergencies and military situations was supported.

Most experts outside the MOD found the method for achieving consensus in relation to the NDS, the Green Book and the NDDP unsatisfactory. For example, the leadership of the MOI felt that they were not engaged in the drafting process. It was also argued that actors were engaged only formally; there was a lack of leadership and no methodological planning instructions; and the classification of threat scenarios inhibited the participation of ministerial experts.

National Defence Development Plan (NDDP) 2013-2022

One positive aspect of the process of drafting the NDDP was the realisation, as explained by one defence expert, that the **MOD, with its hierarchical and clear chain of command, is different from other ministries who sometimes regard themselves as 'advocates of joint ventures vis-à-vis the government' rather than as regulators of their policy areas**,. It also appeared that even in 2012 the ministries were still holding the mistaken view that responsibility for their policy areas would change during different emergency situations (e.g. that ensuring the everyday provision of vital services is normally the responsibility of the MEAC, but would belong to MOI during emergency situations and MOD in wartime). Today, the ministries have largely understood that their roles and responsibilities will not alter in different circumstances. One expert suggested that the fact that the ministries have accepted the need for cross-sectoral long-term planning for wartime activities, while regular planning cycles are normally short-term during peacetime, is a positive step forward.[30] The ministries have also begun to grasp that it is not the military's task to establish criteria for the wartime provision of vital services, but that each ministry must itself determine criteria for the whole of society within their respective policy areas.

Some experts complained that **the plan should have been drafted as a comprehensive document with the equal participation of all ministries**. Today, the military part has been approved by the government, and the other ministries are forced to draw up plans on the conditions it sets out. Some respondents thought that the conceptual foundation of integrated national defence and the need for a comprehensive plan had not been sufficiently explained by the MOD;

[30] The planning cycle for ensuring the continous operation of vital services is short-term (plans are presented to a relevant authority each year) and it does not include planning for states of emergency or wartime. According to the Emergency Act, a risk assessment regarding continuous operation and a continuous operation plan should be reviewed at least once every two years (Riigikogu, 2009; MOI, 2010).

others thought the problem was over-classification, which excluded many working level experts.

One problem area that the experts pointed out is **the need to regulate the readiness of service delivery by the private sector (the providers of vital services) and voluntary actors** during non-military emergency situations and war. For example, the MSA has no legal mandate to oblige privately-owned hospitals (joint ventures) to plan for and allocate resources for managing national emergencies. Fortunately, in practice this has not hindered the management of emergency situations. The same applies in the administrative area of the MEAC with regard to the providers of vital services of special importance for national defence.[31]

Likewise, one expert anticipated that, as the Rescue Board has no mandate to deploy off-duty rescuers, there might be a lack of rescue workers in the case of a major emergency. The number of rescuers at permanent readiness is 350-400: if a greater number is needed, the off-duty personnel may decline to work. The expert recommended that an employment contract should ensure that a sufficient number of rescue workers can be deployed in a national security situation.[32] A shortage of doctors could occur in one region where there has been a massive increase of patients due to a regional emergency, so procedures for transferring doctors from one region to another must be developed.

Voluntary contributions in the defence and internal security domains are currently self-regulated, and more systematic top-down regulation is needed. With regard to voluntary rescue workers, members of the Defence League, and voluntary assistant police officers there is **no central database to provide an overview of the assigned wartime positions of each individual**. The Defence League and the police have informally agreed to start mapping the different organisational affiliations of their voluntary members, which will help to eliminate possible overlaps in planning. The Health Board and the Defence Resources Board should also assign wartime roles to individual doctors and their support personnel. Medical doctors will continue their functions in civil hospitals in wartime; however, measures are needed to ensure that supporting personnel are also not mobilised. At present, exemptions from mobilisation are agreed only for personnel in key coordinating functions, but one expert argued that a wider circle of positions should be exempted so that hospitals could continue their peacetime functions in wartime. For example, an exemption should be made for the Permanent Secretary of the MSA, who has an overall picture of the health care sector.

The MSA has an obligation to ensure that vital services will be available during wartime, and to do so, special operational plans (*toimepidevuse tagamise plaanid*) that are being drawn up, should also consider military threat

[31] The problem can be solved by special laws (e.g. the Health Care Act) or Government or ministerial decrees once the Emergency Act has been amended to update its list of vital services. The MOI plans to present an amendment proposal to the government by the end of 2013 or at the beginning of 2014. The principle that each ministry is responsible for the vital services within its administrative area will not be altered.

[32] The contracts should ensure social security benefits for deployment in emergency situations that pose higher risks to safety.

scenarios.[33] In addition, there is a need to provide regular medical care (general practice) during wartime in order to take the pressure from the emergency services and special doctors, but this issue has not yet been addressed. The weakest link in emergency and wartime readiness in the civilian healthcare system is the functioning of the general practitioners system (*perearstisüsteem*): there is no reserve of general practitioners. A joint military and civilian system would free some resources that could be used to establish a wartime reserve (with the caveat that in wartime, military doctors will not be available for civilian populations).[34]

III.3.8 Pooling and sharing capabilities and interoperability of assets

As every actor tends to defend its independence of action and is unwilling to give up its authority and assets for pooling and sharing, the Government should set out **a roadmap for pooling and sharing and the dual use of assets with clear deadlines and resources**. The roadmap should be based on an independent external assessment.

The Rescue Board has a good overview of the capabilities and assets that the Defence Forces could make available for crisis management and, as explained earlier in this chapter, civil-military interaction in civilian support to the military and in crisis management is good. However, there is a **lack of the material resources (personal equipment, vehicles, etc.) required to support a major incident** (e.g. each rescue unit does not have a reserve vehicle). Additional resources will be needed for the development of those capabilities that are not used every day.

Like strategic planning and the coordination of inter-agency processes, the **narrow mandates and stove-piped interests of the ministries inhibit pooling and sharing efforts.**[35] Another burden crippling pooling and sharing between the MOD, the MOI, and the other ministries **is a lack of working-level coordination due, in turn, to a lack of time and resources** ('we do not have the luxury of coordination'), and rigid and time-consuming bureaucratic and hierarchical ministerial working procedures. A solution would be to **create cross-sectoral coordination mechanisms for particular policy areas** (e.g. energy security, terrorism, cyber security, etc.).

A framework contract on the engagement of the Defence Forces in supporting non-military emergencies is currently being drawn up by the Rescue Board and the Defence Forces. It was stressed that this framework must determine the conditions and practical procedures for using the Defence Forces and their equipment (military vehicles, cranes, air cushions, etc.), including

[33] According to the Peacetime National Defence Act (Riigikogu, 2002/2013), the MSA prepares for and organises medical care during mobilisation and wartime. The NDS states that the vital services for national defence are stationary special medical care, emergency care, and provision of blood supplies. Guidance for drawing up peacetime operational plans is given in a decree of the Minister of the Interior (MOI, 2010).

[34] The impact on internal security of coming emergency medical reform was assessed differently by the MOI (the reform has negative implications) and MSA (the reform has positive implications). It is recommended that the results of this reform should be analysed by the end of 2014.

[35] It was suggested that the new National Defence Act should determine how pooling and sharing should be organised.

outlining lists of capabilities, and points of contacts. Even though civil-military interaction in the dual-use of assets has been good, there have been instances where military assistance was not available on request (e.g. the Defence Forces did not provide vehicles for the transport of euros; the Rescue Board was unable to use air cushions, etc.). One expert also noted that civilian (the Police and the Rescue Board) and military communication equipment (radios) should be compatible, and that there should be a single chain of logistic support (fuel, food, etc.).

III.3.9 Education, training, and exercises

Operational and tactical inter-agency interaction was rehearsed in 2011, when civil protection actors participated in the European Union's Chemical and Radiological Emergency Management Exercise (CREMEX). The scenario involved resolving a radiation, chemical and hostage emergency, including mass evacuation.

All interviewed government officials strongly emphasised that the **political leadership, top and middle-level managers of ministries and government agencies, and heads of municipalities must be educated and trained**. A training course for leadership focused on integrated defence, and tailored seminars, should be conducted regularly. One positive example is the 8-hour module outlining inter-agency civil-military interaction for domestic crisis management conducted during a mid-level staff course at the Baltic Defence College. The MOD has also conducted occasional information briefings for ministries.

A crisis management exercise at the strategic leadership level (including Government ministers) based on realistic scenarios involving many simultaneous security threats (internal and external threats, cyber security, etc.) should be conducted. In addition, more joint training and exercises for the defence and rescue forces should be conducted to practice emergency situations. Exercises should be designed to test practical cooperation mechanisms in limited areas, rather than table-top exercises where all parties agree in principle, but where actions are not carried out in real physical settings.

Host Nation Support exercises that involve the health care system have been extremely useful for their personnel, but a wider circle of participants should be engaged (e.g. all health care actors who make decisions at the working level in times of emergency).[36]

It was suggested that the **rotation of working-level civil servants** between the military and civilian spheres would be complicated, because there is normally just one person on the civilian side responsible for domestic emergency issues, and national defence issues comprise only a tiny part of their duties: qualification and competency requirements for rotating personnel would thus be high.

[36] It was suggested that because the health care sector does not have capacity (and resources to create such capacity) to organize exercises across the health care sector, a central authority should run regular inter-agency exercise cycle.

III.3.10 Comprehensive approach in international cooperation

Inter-agency process regarding the deployment of Estonian troops, staff officers, and civilians in international missions is normally **ad hoc and based on personal relations**. It was evident from the interviews that depending on such networks **reduced accountability and transparency in decision making**. The leadership of the ministries were not clear how decisions were made, they noted a lack of information exchange, and that key actors are not engaged early enough in the planning and preparation of draft laws concerning international missions. It was stressed **that some decisions are made in exclusive narrow circles** (indicating that the decision makers do not remain open to opposing views).[37]

It was suggested that in the preparation of draft acts to be presented by the Government to the Parliament concerning the deployment of Estonian troops in international missions, **other government ministries should be engaged earlier, during the planning stage** (there have been cases in which planned changes concerning the deployment of Estonian troops have not been communicated to other ministries). Other ministries do not recognise political gains from the contribution of Estonian troops or staff officers to international missions.

One respondent explained that while planning of civil participation in international operations takes place on an ad hoc and personal relations basis, it remains **questionable whether formalisation and institutionalisation would help to solve problems**. It was pointed out that hospitals are reluctant to allow qualified surgeons to leave their jobs for deployment in international missions, as this results in an absence from work of more than three months. The deployment of top surgeons to international missions provides experience and helps to develop the emergency and wartime capabilities needed for internal/domestic defence, as well as supporting Estonia's foreign policy goals. In some areas of medical care in Estonia, there are only a couple of top specialists and their priority and duty is to assist the Estonian population. If the military would like to deploy more surgeons to international missions, more specialists should be educated. The leadership of hospitals has, however, become more supportive of doctors who seek to gain mission experience.

For many years there has been a problem in the provision of weapons for police officers who are deployed to international missions abroad; they will lose their legal status as policemen and the MFA, who recruits them, does not want to handle guns. While the MOI believed the legal basis has not been changed due to the different understandings of the ministries, the MFA felt that this was a technical problem. Whatever the reason, this issue has not been solved over the years.

[37] Institutionalized networks are a means to build an organization's social capital, where ties are formed between the institutions and government bodies, civil society groups, thought leaders, individuals. OECD Public Governance Reviews: Estonia (OECD, 2011:120).

Part III Conclusions

This part of the report has described the main policy documents of and institutional architecture for Estonia' integrated national defence. Based on interviews with key government experts, incentives for and obstacles to the application of a whole-of-government approach have been identified. The need to implement integrated national defence has been widely accepted and supported across all government actors. The everyday operational inter-agency interaction in crisis management and in the area of civilian support to the military is good, even though greater formalisation and regulation of interaction, and more practical inter-agency training and exercises, is needed in some policy areas. A number of best practices were outlined (civilian support to the military, the inter-agency risk assessment procedure, the Defence League) that can be further studied for possible application in other functional policy areas.

The key obstacles to the implementation of whole-of-government and whole-of-society approaches are rigid and outdated mindsets and divergent philosophical understandings across the ministries and their sub-agencies concerning the essence of integrated national defence; a lack of strategic and long-term planning traditions, procedures, regulations and instructions across all governance domains and policy subjects; a lack of competence, know-how, and human and financial resources that inhibits strategic planning efforts; and insufficient coordination of inter-agency plans and processes. The deficiencies with the gravest negative implications for national security are the lack of preparation for the assumption of wartime responsibilities and duties (no legal mandate, attribution of financial resources, and no strategic and operational planning in some policy areas); and a lack of clarity regarding the leadership and command structure during various stages of escalation (emergency situation, state of emergency, wartime).

Key Insights from Part III

- There is an **overall consensus and acceptance** of the principles and objectives of integrated national defence; however, academic and whole-of-society discussion on a strategic vision for integrated national defence is needed.
- The current conceptual and strategic documents are **not suitable as guidelines for strategic planning**.
- **Estonia's governance structure and culture inhibits** cross-sectoral policy planning and implementation.
- **Education** about the existing civilian and military procedures and arrangements, and about future development plans in the entire security sector (including defence) should be conducted to raise awareness among both civilian and military actors.
- Factors that contribute to a **weak strategic planning** capability are:

  - The lack of a central integrating authority, weak planning habits, and uncertainty on mid- and long-term financial resources in policy areas other than defence;
  - The lack of strategic long-term planning traditions, practical guidance and in-depth expert knowledge;
  - The lack of information exchange between actors about planning and other initiatives;
  - Little coordination and collaboration in developing ministerial development plans.

- There are many **success stories in inter-agency cooperation and collaboration**: the risk assessment procedure, civilian support to the military, the activities of the Defence League.
- **Earlier engagement** of non-government stakeholders and more inter-agency consensus will be needed in developing legal acts and policies on cross-sectoral policy subjects.
- A number of policy issues remain to be solved **by amending or enacting legal acts** (establishing a legal mandate to ensure voluntary and private sector contributions in major emergencies and in wartime ensuring effective pooling and sharing of capabilities, etc.).
- Factors that **constrain collaboration at the strategic level** are: the different expectations and mistrust that result from a lack of information; the ministries' unwillingness to give up some independence and authority.
- Although operational day-to-day inter-agency interaction is fairly good, the **current decentralised system of managing it is rather ineffective and inefficient**, containing potential points of failure (e.g. due to the lack of alignment of geographical areas of responsibility of various agencies with the regional crisis management structure).
- There is some **confusion regarding leadership and command structures** during different stages of crisis escalation.
- Decision-making concerning involvement in **international operations** lacks formal and inclusive process of consultation and decision-making.

Final Conclusions and Recommendations

This report has explored the challenge of building a comprehensive security and integrated defence system. First, on the basis of a literature review, it has identified various conditions at the national, governmental, agency, team and individual levels that are required for successful interaction among security and defence stakeholders. Such interactions – especially in the advanced form of collaboration – lie at the heart of whole-of-government and whole-of-society models. Implementing these models requires broad changes, including in governance culture and institutional structures, in inter-agency processes and working practices, and in leadership styles and individual skills. Committing to develop a whole-of-government / whole-of-society approach is obviously an ambitious undertaking with very broad implications for how security and defence affairs should be conducted.

Given the scope of this challenge, it is not surprising that many countries are making a rather slow progress towards effective whole-of-government and whole-of-society approaches to security and defence. This report has looked at how four nations – Denmark, Finland, the Netherlands and Sweden – pursue such approaches and has found the picture to be mixed at best. Governance traditions, entrenched bureaucratic cultures, structural legacies and other factors often conspire against more rapid and effective change. However, there is a host of good, if not best, practices that are worth emulating in Estonia. Denmark demonstrates the value of a sustained political consensus on defence policy and of the importance of harnessing internal resources for comprehensive external action; Finland is a prime example of a how total defence legacy can be successfully adapted to an age of comprehensive security; there is much to learn from the Netherlands' sophisticated, systematic and methodical approach towards comprehensive planning; while Sweden demonstrates the importance of clarity in the underlying principles and functioning of the crisis management system.

In many regards, Estonia does not appear to be a laggard in pursuing its own whole-of-government/whole-of-society solutions. This report has also investigated the 'state of play' in Estonia in one particular area of interest – integrated defence – and demonstrated that the picture is not black and white. The conceptual basis – the understanding of how complex and dynamic the threat environment is and the requirement for an integrated application of the resources and tools available to the nation to deal with it – is in place, if in need of some fine-tuning. Many legal, institutional and organisational elements are also emerging, reinforced by the positive experiences of operational interaction, including the involvement of the non-government and private sectors.

However, there are many weaknesses too, concentrated primarily in the areas of:

- **strategic planning culture, and institutional competence and arrangements** for whole-of-government/whole-of-society approaches, as many organisations are driven by short-term budgetary cycles, do not have elaborate medium- and long-term

capability planning systems, and are guided mostly by their own narrow interests in a decentralised institutional environment;

- **availability and management of human resources**, especially of those with deep competence in strategic planning disciplines, working experience in many security and defence sector organisations, and skills of integrating diverse inputs from various stakeholders into coherent strategies and plans;
- **knowledge management**, especially in maintaining broad awareness of what various organisations do and plan for, in translating the implicit knowledge residing with individuals into explicit knowledge through manuals, handbooks and guidelines (which hampers 'business continuity') and in generating and implementing system-wide 'lessons learned';
- **management of inter-agency processes in security and defence** (both in planning stages and crisis situations), with too much of ad hoc cooperation based on personal relations and informal networks, and too little of structured, systematic and sustained inter-agency co-ordination and collaboration;
- **management of stakeholder expectations** (e.g. concerning the funding sources for integrated defence preparedness measures, leadership roles in various processes, etc.).

Resolving the issues in the above areas will take time, sustained effort, patient leadership and the good will of all stakeholders. In some cases, the imperative of building a more coherent and effective comprehensive security and integrated defence system may collide with tenets currently central to how Estonia is governed (e.g. 'lean state' with a small administrative apparatus; independence of ministries, etc.). But, with some creativity, modern managerial and technical tools and, most importantly, a genuinely whole-of-society approach, such collisions need not impede progress in putting into practice the concepts of comprehensive security and integrated defence.

On the basis of the report's findings, it is recommended that the Parliament and the Government of Estonia should seek to:

1. Promote a **broad debate** on the conceptual and practical aspects of whole-of-government and whole-of-society approaches to security and defence, in order to achieve a greater degree of common understanding and consensus among various stakeholders.

2. Through educational programmes (such as the Higher Defence Course), **continue to raise awareness** in security and defence stakeholders of the institutional arrangements, mechanisms and measures needed to ensure effective whole-of-government/whole-of-society collaboration, and of the policies, practices, capabilities and working methods of various agencies.

3. Significantly **enhance the role of the Government's Office** as the central authority with overarching responsibility to co-ordinate and integrate cross-sectoral policies and plans in security and defence and oversee their implementation, in support of the Government's National Security Committee.
   3.1. The **legal mandate** of the Government's Office should be expanded to ensure that it has the authority to guide and coordinate the ministries in conducting strategic planning for security and defence and to oversee progress in implementation.
   3.2. This mandate should also direct the Government's Office to provide advice to the entire National Security Committee, not only the Prime Minister, and to make substantive inputs to its agenda.
   3.3. Establish **formal procedures** for formulating the agenda of the Committee, enacting its decisions and communicating these to various stakeholders, and monitoring the implementation of those decisions.

4. Appoint **heads of preparedness** in all ministries and agencies and establish a regular format for them to meet, headed by the Government Office.

5. Streamline **whole-of-government decision-making arrangements for cross-sectoral policies** at the Government level by introducing the following structure:
   5.1. **Political level**: Government's National Security Committee, to deal with crisis management, security and defence issues;
   5.2. **Senior executive level**: a single integrated crisis, security and defence council (instead of the current multiple councils and commissions), staffed by the permanent secretaries of the ministries and the heads of the relevant agencies, and tasked with executive co-ordination of all cross-sectoral policies, plans, resources and implementation measures;
   5.3. **Expert level**: permanent expert panels of government, non-government and private sector experts and heads of preparedness (co-ordinated by 'issue coordinators' from the Government's Office), to provide expert inputs to the National Security Committee.
   5.4. **Regional level**: expand the mandate of the current regional crisis committees to cover all cross-cutting security and defence issues within their specified geographical area (region). Turn them into the main platforms for operational collaboration in cross-cutting security and defence issues in that particular area.
      5.4.1. To the extent possible, align the activity boundaries of all agencies with the boundaries of the regional crisis committees.

6. Engage **all relevant stakeholders, especially from the non-government and private sectors** early on when crafting cross-sectoral policies and plans.

7. While earmarking 2% of GDP for defence purposes, ascertain that this is, in line with NATO definitions, directed towards military defence and the development of military capabilities. However, to enable organisations other than the MOD to develop various measures and capabilities to perform their tasks during crisis and war, consider setting up a separate (i.e. not within the defence budget) dedicated **trust fund to finance crisis and war preparedness projects and activities**.
   7.1. This fund should be managed by the Government's Office.
   7.2. The fund should be **available not only to government agencies but also to non-government and private sector organisations** with roles in comprehensive security and integrated defence (e.g. hospitals, companies in charge of vital infrastructure, NGOs working in the field of psychological support to the population, etc.).
   7.3. As a fund designed to finance non-military aspects of integrated defence, it would be entitled to apply for **EU funding** aimed at enhancing societal security and resilience.
   7.4. This trust fund could be either **permanent or temporary**. A permanent trust fund would, to a certain extent, relieve government organisations from their responsibilities for crisis and war preparedness and could therefore hamper long-term development. Instead, a temporary solution could act as a catalyst and enabler for these organisations to launch long-term planning activities and preparedness projects. At a later stage, funding would take place within the annual budget of each ministry responsible for a particular sector of comprehensive security and integrated defence.

8. Establish, under the Government's Office, a **capacity-building programme** to strengthen the strategic planning competences and capacities of government and non-government organisations working in the field of crisis management, security and defence.

9. Draw **a clear set of doctrinal principles** and **standard operating procedures** governing stakeholder interactions (particularly for coordination and collaboration as the most advanced forms) in security and defence, including in strategic planning, pooling and sharing of capabilities, and in learning and applying lessons. As an example of the principles:
   9.1. The principle of **responsibility**: that whoever is responsible for an activity in normal conditions should maintain that responsibility, and initiate cross-sectoral actions, during crisis.
   9.2. The principle of **proximity**, whereby a crisis is to be handled in the area in which it takes place, and be managed by those most closely affected and responsible. Crisis management should only be referred to higher levels if it is considered necessary.

9.3. The principle of **continuity**, which means that an organisation's activities and location should, as far as possible, be kept the same during a crisis. Changes to an organisation should be no larger than necessary in order to handle the crisis.

10. Clarify, in legal acts and inter-agency doctrine, the **roles and responsibilities** of various actors as well as **command and control arrangements** for the entire spectrum of crisis, from emergency situation to wartime.

11. Provide more **training and practical exercises** dealing with cross-cutting security and defence challenges for all actors, at all levels (political, senior executive, expert and regional).
    11.1. Ensure that these exercises are **regular** and their **lessons learned are formalised and incorporated** into the preparedness of all agencies.

12. Establish a permanent inter-agency expert panel (as one of the expert level groups suggested earlier) to provide guidelines for and supervise **technical integration** efforts, and address **interoperability issues** between security and defence organisations.

13. Better utilise the **Estonian Academy of Security Sciences**, which already serves multiple end-users – security and safety agencies – as a platform for inter-agency training, education and research, especially in collaboration with the **Estonian National Defence College**. Both organisations have to be better resourced to perform this role.

14. Consider introducing **rotation, exchange and liaison programmes for public servants** to facilitate their acquisition of multi-organisational awareness, experiences and perspectives across the security and defence sector.

References

Part I

Baumann, A B *The UK's Approach to Stabilisation: The Comprehensive Approach in Action?* International Security Programme: Rapporteur Report (London: Chatham House), 2010.

Baumann, A B *Silver bullet or time suck? Revisiting the role of interagency coordination in complex operations*. Prism Vol. 3, No. 3, 2012, pp. 33-46.

BBC News. 'German army's crisis role widened', 17 August 2012 [http://www.bbc.co.uk/news/world-europe-19295351] (21.08. 2013).

Bryan, E L & Pendall D *We are interagency: Exercising a Comprehensive Approach to crisis action and conflict termination and stabilization.* Interagency Essay, No. 10-02, 2010.

Caslen, R L & Loudon, B S *Forging a comprehensive approach to counterinsurgency operations*. Prism, Vol. 2, No. 3, 2011, pp. 3-14.

Davidson, L W, Hayes M D, Landon, J J *Humanitarian and Peace Operations: NGOs and the Military in the Interagency Process* (Washington D.C.: NDU Press), 1996.

Egnell, R *Civil-military coordination for operational effectiveness: Towards a measured approach*, *Small Wars & Insurgencies,* Vol. 24, No.2, 2013, pp. 237-256.

Fitz-Gerald, A & Macnamara, D *Comprehensive Security Requires Comprehensive Structures – How Comprehensive Can We Get?* Strategic Studies Working Group Papers (Ottawa: Canadian Defence & Foreign Affairs Institute and Canadian International Council), 2012.

Fox, J E *Preparing civilians for deployment to civilian-military platforms in combat environments: The evolution of staffing and training for the civilian mission in Afghanistan*, in Schnaubelt C. M. (ed.). Towards a Comprehensive Approach: Strategic and Operational Challenges. NDC Forum Paper 18 (Rome: NATO Defence College),2011, pp. 41-68.

Friis, K *The Politics of the Comprehensive Approach: The Military, Humanitarian and State-Building Discourses in Afghanistan*. NUPI Working Paper 773 (Oslo: NUPI), 2010.

Hallett, M & Thorngren, O *Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development*, in Neal D. J. & Wells II N. (eds.). Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions (Washington D.C.: NDU Press), 2011, pp. 35-50.

Hull, C *Focus and Convergence through a Comprehensive Approach: but which among the many?* Swedish Defence Research Agency, 2011.

Jennings, C A *All for one and one for all? Forging development, diplomatic and defense partnerships under NATO's new Strategic Concept*, in Schnaubelt C.M. (ed.), Towards a Comprehensive Approach: Integrating Civilian and Military Concepts of Strategy. NDC Forum Paper 15 (Rome: NATO Defence College), 2011, pp. 89-114.

Lacquement, R A *Integrating civilian and military activities.* Parameters, Vol. 41, Issue 4, 2011-2012, pp. 1-12.

Lindley-French, J *Operationalizing the Comprehensive Approach.* Atlantic Council Issue Brief, 2010.

Lira, L *An integrative approach to the interagency process.* Interagency Journal, Vol. 1, Issue 1, 2010, pp. 46-54.

Lutterbeck, D *Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe*. *European Security,* Vol. 14, Issue 2, 2005, pp. 231–253.

Miani, L *Unlocking interagency secrets: A new rosetta stone?* Interagency Journal, Vol. 1, Issue 1, 2010, pp. 10-18.

Organisation for Economic Cooperation and Development (OECD) *Estonia: Towards a Single Government Approach,* OECD Public Governance Reviews (Paris: OECD Publishing), 2011.

Petersen, F A, Binnendijk H *The Comprehensive Approach initiative: Future options for NATO*. Defense Horizons, No. 58, 2007 pp. 1-5.

Prevent Project. *Beyond Pandemics: A Whole-of-Society Approach to Disaster Preparedness.* Towards a Safer World: Practical Approaches to Advance Disaster Preparedness, 2011

Rotmann, P *Built on shaky ground: The Comprehensive Approach in practice*. Research Paper No. 63 (Rome: NATO Defence College), 2010.

Schnaubelt, C M *The challenges to operationalizing a Comprehensive Approach*, in Schnaubelt C.M. (ed.). Operationalizing a Comprehensive Approach in Semi-Permissive Environments. NDC Forum Paper 9 (Rome: NATO Defence College), 2009, pp. 35-67.

Stepputat, F *Integrated National Approaches to International Operations: The Cases of Denmark, UK, and the Netherlands.* DIIS Report 2009:14 (Copenhagen: DIIS).

Strickler, T *Interagency cooperation: Quo vadis?* Interagency Journal, Vol. 1, Issue 1, 2010, pp. 3-9.

Waddell, R *A perspective on cultural clash and organizational change in Iraq: Smart power in action?*, in Schnaubelt C. M. (ed.). Towards a Comprehensive Approach: Strategic and Operational Challenges. NDC Forum Paper 18 (Rome: NATO Defence College), 2011, pp. 8-40.

Van de Goor, L, Major, C *How to make the comprehensive approach work: Preparation at home is key to effective crisis management in the field*. CRU Policy Brief #21, 2012.

Part II

II.1 Denmark

Breitenbauch, H O *Kompas og Kontrakt: For en dansk sikkerhedsstrategi*, DIMS Report May 2008, [http://cms.polsci.ku.dk/pdf/kompas_og_kontrakt.pdf]

Breitenbauch, H O *Beredskab eller intern sikkerhed? Danmark og den internationale institutionsudvikling inden for det robuste og sikre samfund*, CMS Report 2012, May 2012, [http://cms.polsci.ku.dk/pdf/pub/Beredskab_eller_intern_sikkerhed_H_B.pdf/]

Bruun udvalget 'De sikkerhedspolitiske vilkår for dansk forsvarspolitik', August 2003, [http://www.drv.dk/upload/fb__4628_12201.pdf].

Danish Security and Intelligence Service 'PET påbegynder partnerskabsprogram i Kenya', 2012, [https://www.pet.dk/Nyheder/2012/PET%20paabegynder%20partnerskabsprogram%20i%20Kenya.aspx]

Danish Security and Intelligence Service 'Center for Terroranalyse (CTA)', 2013, [https://www.pet.dk/CTA.aspx]

Defence Command Denmark *Forsvarskommandoen Årsrapport 2012*, [http://www.fmn.dk/videnom/Documents/aarligredegoerelse/FKO_aarsrapport_2012.PDF].

Fischer K, Top Christensen J ' Improving civil-military cooperation the Danish way', 2005, http://www.nato.int/docu/review/2005/issue2/english/special.html

Grube, C 'The international Situation and Danish Foreign Policy', Hvidt, N, Mouritzen H (eds.) *Danish Foreign Policy Yearbook 2013*, Danish Institute for International Studies,

2013 [http://subweb.diis.dk/graphics/Publications/Books2013/YB2013/YB2013-02_Claus_Grube_web.pdf].

Home Guard 'Virksomhedshjemmeværnet - Det sårbare samfund', 2013, [https://www.hjv.dk/VHV/Om%20Virksomhedshjemmev%C3%A6rnet/Sider/Velkommen.aspx]

Ministry of Defence *Defence Commission of 2008* (presentation page), 2013a [http://www.fmn.dk/eng/allabout/Pages/DefenceCommission2008.aspx]

Ministry of Defence 'Prior Danish Defence Agreements', 2013b [http://www.fmn.dk/eng/allabout/Pages/Prior-Danish-Defence-Agreements.aspx]

Ministry of Defence 2004a 'Danish Defence Agreement 2005-2009', [http://www.fmn.dk/eng/allabout/Documents/ENG_Forligstekst.pdf]

Ministry of Defence 2004b 'The Mandate of the Task Group Regarding the Transfer of the National Emergency Management Agency under Danish Defence', [http://www.fmn.dk/eng/allabout/Documents/ENG_Kommissoriumforarbejdsgruppe.pdf]

Ministry of Defence *Summary. Danish Defence Global Engagement. Report by the Danish Defence Commission of 2008*, 2009, [http://www.fmn.dk/videnom/Documents/Summary-Report_Danish_Defence_Commission_June2009.pdf]

Ministry of Foreign Affairs of Denmark *Peace and Stabilisation. Denmark's policy towards fragile states 2010-2015*, 2010, [http://amg.um.dk/en/~/media/amg/Documents/Policies%20and%20Strategies/Stability%20and%20Fragility/Peaceandstabilisation.ashx]

Ministries of Foreign Affairs, Defence and Justice *Danmarks samtænkte stabiliseringsindsatser i verdens brændpunkter*, September 2013, [http://um.dk/da/~/media/UM/Danish-site/Documents/Politik-og-diplomati/Nyheder_udenrigspolitik/2013/Danmarks%20samtaenkte%20stabiliseringsindsatser%20i%20verdens%20braendpunkter.pdf]

Ministry of Foreign Affairs of Denmark/Danish Ministry of Defence 'Samtænkning af civil og militær indsats i internationale operationer', 2004, [http://www.fmn.dk/SiteCollectionDocuments/FMN/Forsvarsforlig%202005%202009/Samt%C3%A6nkning.pdf]

Ministry of Foreign Affairs of Denmark/Danish Ministry of Defence *Denmark's Engagement in Afghanistan 2008-2012*, 2008, [http://www.netpublikationer.dk/um/9103/pdf/Afghanistan_pixie_engelsk.pdf]

Ministry of Foreign Affairs of Denmark/Danish Ministry of Defence *The Afghanistan Plan 2013-2014. Towards full Afghan responsibility*, 2013, [http://www.fmn.dk/eng/news/Documents/The-Danish-Afghanistan-Plan2013-2014.PDF]

Regeringen *Et Danmark, der står sammen*, Regeringsgrundlag [Government plan], October 2011 [http://www.stm.dk/publikationer/Et_Danmark_der_staar_sammen_11/Regeringsgrundlag_okt_2011.pdf]

Schmidt, S *Afghanistan. Organizing Danish Civil Military Relations.* DIIS Report 1009:15, [http://subweb.diis.dk/graphics/Publications/Reports2009/DIIS_Report_2009_15_Afghanistan_web.pdf]

Statsministeriet *Links to former Government plans*, November 2013, [http://www.stm.dk/_a_3023.html]

Stepputat, F *Synthesis Report: Civil-Military Relations in International Operations. A Danish Perspective*, DIIS Report 2009:16, April 2009, [http://subweb.diis.dk/graphics/Publications/Reports2009/DIIS_Report_2009_16_Synthesis_Report_web.pdf]

Søby Kristensen K, Salling Larsen E *At lære for at vinde. Om dansk militær erfaringsudnyttelse i internationale operationer*, DIMS Report Marts 2010, [http://cms.polsci.ku.dk/pdf/atlaereforatvinde.pdf/]

II.2 Finland

Ministry of Defence, *The Security Strategy for Society,* Government Resolution, 2011. [http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/26-security-strategy-for-society]

II.3 The Netherlands

Spoelstra M, van Bemmel I E, Eikelboom A R, 'Comprehensive Planning in Complex Endeavours', TNO Defence, Security and Safety, 2010.

Van Bemmel I E, Eikelboom A R, 'The Comprehensive Planning in Uruzgan', *15th ICCRTS 'The Evolution of C2',* 2010.

The Netherlands Ministry of Defence & The Netherlands Ministry of the Interior and Kingdom Relations, 'Civil-Military Cooperation', 2007.

The Netherlands Ministry of Foreign Affairs, 'A Secure Netherlands in A Secure World', *International Security Strategy,* June 2013 [http://www.government.nl/ministries/bz/documents-and-publications/notes/2013/06/21/international-security-strategy.html]

The Netherlands Ministry of the Interior and Kingdom Relations, *National Security Strategy and Work Programme 2007-2008,* May 2007.

Wittkowsky A, Wittkamp U, 'Pioneering the Comprehensive Approach: How Germany's Partners Do it', Policy Briefing, Centre for International Peace Operations (ZIF), January 2013. [http://www.zif-berlin.org/fileadmin/uploads/analyse/dokumente/veroeffentlichungen/ZIF_Policy_Briefing_Andreas_Wittkowsky_Ulrich_Wittkampf_Jan_2013.pdf]

II.4 Sweden

2005 års katastrofkommission. *Sverige och tsunamin - granskning och förslag*. Statens offentliga utredningar, 2005.

Bergrum.se *Krigsproduktion.* (webpage). [http://www.bergrum.se/sverige/ekonomiskt/produktion.html]

Försvarshögskolan (FHS) *Krishantering.* (webpage). [http://www.fhs.se/sv/utbildning/uppdragsutbildningar/krishantering/] (15.11.2013).

FHS, *Vägen mot ett nytt civilt försvar. Ett förslag till handlingsplan. Reviderad och utvecklad rapport utarbetad av Försvarshögskolan på uppdrag av Myndigheten för samhällsskydd och beredskap*, 2013.

Government Offices of Sweden *The Government at work.* (webpage). [http://www.government.se/sb/d/2856/a/18335] (11.11.2013).

Government Offices of Sweden. *Crisis Management Coordination Secretariat.* (webpage). [http://www.government.se/sb/d/3778/a/129557] (11.11.2013).

Hedström L On comprehensive security in Sweden. [interview] Stockholm, 07 November 2013.

Hurt M *Laiapõhjaline riigikaitsemudel - analüüs ja võrdlus teiste riikide näitel: Riigi juhtimine tava-, häda- ja sõjaolukorras.* International Centre for Defence Studies. Tallinn, 2011.

MSB, *Överenskommelse om kommunernas krisberedskap*. SKL 12/6159, 2012-5541. Stockholm, 2013.

MSB, *Området samhällsskydd och beredskap (skydd mot olyckor, krisberedskap och civilt försvar).* Powerpoint presentation.November, 2013.

MSB, *Inriktning för området samhällsskydd och beredskap. Andra delrapporteringen*, 2012.

MSB, *Utgåva 1 av Strategi för civilt försvar - beslutad att gälla under 2012 som underlag för arbetet med konceptutveckling och försvarsplanering*. 2012b.

MSB, *Handling serious IT incidents. National Response Plan, interim version*, 2011.

MSB, *Interorganisatorisk samverkan som nationell resurs i krishanteringen*,2007.

Riksdagen, *Regeringsformen. Kungörelse om beslutad ny regeringsform,* 1974:152*.*

Regeringskansliet Försvarsdepartementet, *Vägval i en globaliserad värld,* 2013.

Regeringskansliet, *Krishantering i Regeringskansliet. Rapport från utredaren Christina Salomonson om inrättandet av en nationell krishanteringsfunktion i Regeringskansliet*, 2007.

Riksdag. *Förordning om krisberedskap och höjd beredskap (2006:942).*

Riksdag. *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.* 2006:544.

Riksdag. *Lag om totalförsvar och höjd beredskap*. 1992:1403.

MSB-Swedish Civil Contingencies Agency (webpage). [https://www.msb.se/en/] (11.11.2013).

Werger S. Director of Communications, MSB. On comprehensive security in Sweden from MSB's perspective.[interview] Stockholm, 07 November2013.

Part III

Ministry of Defence (MOD), *National Defence Strategy,* 2010 [http://www.kmin.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf]

Ministry of the Interior (MOI), *Toimepidevuse plaani koostamise juhend (Guidelines for the formulation of continous operation plans)* (RT I 2010, 33, 180), 2010 [https://www.riigiteataja.ee/akt/13326401]

Organisation for Economic Cooperation and Development (OECD). *Estonia: Towards a Single Government Approach,* OECD Public Governance Reviews (Paris: OECD Publishing), 2011.

Riigikogu , *Eesti riigi kaitsepoliitika põhisuundade heakskiitmine* (*Main Directions of the Estonian National Defence Policy*), 1996. [https://www.riigiteataja.ee/akt/13009161]

Riigikogu, *Emergency Act* (RT I 2009, 39, 262), 2009 [https://www.riigiteataja.ee/en/eli/530102013054/consolide]

Riigikogu, *National Security Concept of Estonia,* 2010 [http://www.kmin.ee/files/kmin/img/files/National_Security_Concept_of_Estonia.pdf]

Riigikogu, *Peacetime National Defence Act* (RT I, 20.03.2013, 1), 2002 / 2013 [https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/511112013018/consolide]

Riigikogu, *Sõjaaja riigikaitse seadus (Wartime National Defence Act)* (RT I, 10.07.2012, 33), 1994 / 2012 [https://www.riigiteataja.ee/akt/110072012033?leiaKehtiv]

Riigikogu, *State of Emergency Act* (RT I, 29.12.2011, 208), 2011 [https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530122013002/consolide]

Appendix

Essex-Lopresti T (ed) *A Brief History of Civil Defence.* UK Civil Defence Association, 2005. [http://www.civildefenceassociation.org.uk/HistCDWebA5V5.pdf]

Elomaa T, Halonen A *EUROBALTIC Survey: Civil Protection Research in the Baltic Sea Region.* Aleksanteri Institute, University of Helsinki, 2007. [http://www.helsinki.fi/aleksanteri/civpro/publications/EurobalticII_Civil_Protection_Research.pdf]

NATO Standardization Agency, *NATO Glossary of Terms and Definitions.* AAP-6, 2012.

International Standards Organisation (ISO) *Societal Security: Guideline for incident preparedness and operational continuity management.* ISO/PAS 22399, 2007. [https://www.iso.org/obp/ui/#iso:std:iso:pas:22399:ed-1:v1:en]

Estonian Government, *Eesti sõjalise kaitse strateegia (Estonian Military Defence Strategy),* 2001.

Mendershausen H *Territorial Defense in NATO and Non-NATO Europe.* RAND Corporation, 1973. [http://www.rand.org/content/dam/rand/pubs/reports/2006/R1184.pdf]

Defence Command Denmark, *The Danish Defence Agreement 2005-2009.* [http://forsvaret.dk/FKO/eng/Defence%20Agreement/Pages/default.aspx]

Riigikogu, *Emergency Act* (RT I 2009, 39, 262), 2009 [https://www.riigiteataja.ee/en/eli/530102013054/consolide]

Riigikogu, *National Security Concept of Estonia,* 2010 [http://www.kmin.ee/files/kmin/img/files/National_Security_Concept_of_Estonia.pdf]

Appendix: Terminology

Term	Defined in Estonia as	Defined outside Estonia as	Comments
Civil Defence	An essential part of national defence that involves both the timely notification of the population as well as the application of measures required to protect the population. Issues that contribute to civil defence are taken into consideration at all levels of national defence (MOD, 2010)	Preparation for and actual non-combatant assistance to individuals, groups or communities in need of immediate assistance as a result of natural or man-made events... (Essex-Lopresti, 2005)	Civil Defence is increasingly replaced by the term 'Civil Protection', in recognition that preparedness of and assistance to a civilian population is necessary not only in wartime, but also as a result of other events (see Elomaa & Halonen, 2007). Thus, in essence, this term is converging with what is referred to as 'Crisis Management' in Estonia (see below). It is unclear, however, if the Estonian definition of Civil Defence goes beyond protection of civilians in the event of a military attack. Its definition in the NDS suggests that the concept remains part of thinking about defence only in military contingencies and not in a 'civil protection' sense.
Comprehensive Security	Approach according to which all the factors influencing the nation's security are considered. Its implementation encompasses all the sectors vital to ensuring national security. The main directions of broad-based security are foreign policy, defence policy, internal security policy, cohesion and resilience of society. The broad concept of security entails enhancement of the mutual co-operation of state authorities as well as international co-operation, and the involvement of other members of society in reinforcing security (Riigikogu, 2010).	The end-state of a nation's security policy achieved through the coordinated application of the multiplicity of government and non-government components and instruments involved in developing and maintaining a stable and peaceful environment that permits the effective operation of political, economic and social institutions for the overall benefit of citizens (Fitz-Gerald & Macnamara, 2012: 4).	Both definitions emphasise the concerted actions of governmental and societal stakeholders to ensure national security in multiple sectors.

Crisis Management	A system of measures which includes preventing an emergency, preparing for an emergency, resolving an emergency and mitigating the consequences of an emergency (Riigikogu, 2009).	The coordinated actions taken to defuse crises, prevent their escalation into an armed conflict and contain hostilities if they should result (NATO Standardization Agency, 2012).	The Estonian definition concerns domestic events, while NATO (and, as a result of adopting NATO standards, the definition used in the Estonian military), focuses on 'out-of-area' conflicts. Indeed, the term 'crisis' remains undefined in current Estonian concepts and legislation.
Emergency	An event or a chain of events which endangers the life or health of many people or causes major proprietary damage or major environmental damage or severe and extensive disruptions in the continuous operation of vital services and resolving of which requires the prompt co-ordinated activities of several authorities or persons involved by them (Riigikogu, 2009)	Sudden, urgent, usually unexpected occurrence or event requiring immediate action. An emergency is usually a disruptive event or condition that can often be anticipated or prepared for but seldom exactly foreseen (ISO, 2007)	The Estonian definition does not consider war or a military attack to be an emergency. In the spirit of Integrated Defence, however, it would be natural to suggest that the Crisis Management (see above) system is extended to cover the management of a comprehensive response to war or a military attack as a form of emergency.
Integrated Defence	Approach that encompasses all the options available to the state authorities and the people to ensure the nation's security in the case of military activity against Estonia (Riigikogu, 2010). In case of military action against Estonia, the national defence system will be implemented comprehensively, consisting of military defence, civil contribution to military defence, international activity, ensuring of internal security, securing the resilience of critical services, and psychological defence (MOD, 2010)	No corresponding term has been identified outside Estonia	This term is often referred to as 'broad-based defence' in Estonia. In essence, it is Total Defence (see below). Just as total defence, it is centred on countering an external military threat in different domains. As part of comprehensive security, it relies on similar principles to organise the nation's response; it does not, however, cover the overall response to peacetime non-military emergencies.

Territorial Defence	A principle <...> which means that defence encompasses the territory of the whole state and where great attention is devoted to the defence of strategically important objects. <...> National defence is organised by division of the territory of state to defence districts and each district is divided into defence regions (Estonian Government, 2001).	Defense of a country by a dense network of latent (mobilization-dependent), relatively lightly armed, locally assigned forces. Territorial defense forces are armed forces under the command of military authorities, although by the nature of their tasks these forces must be more closely coordinated with civilian authorities on various levels than is the case for mobile strike forces. <...> In a sense, territorial defense stands between main battle forces and civil defense system, and its resources and functions are linked to both (Mendershausen, 1973: 1-2).	At the strategic level, Territorial Defence denotes the use of armed forces in defence of a national territory against a military attack, in contrast to the use of armed forces in expeditionary operations outside a national territory. This is the most common use of the term today. At the operational and tactical level, it is a doctrinal concept defining how the armed forces are organised and conduct their operations on a national territory; it is an alternative or supplement to mobile (manoeuvre) defence, point defence, frontier defence and other doctrinal concepts. At both levels, it is often used in conjunction with the Total Defence concept (i.e. one does not exclude the other).
Total Defence	In accordance with the principle of total defence, all means will be employed to anticipate and prevent any possible military action against Estonia (MOD, 2010).	Total defence encompasses the utilisation of all resources in order to maintain an organised, functional society and to protect the population and the national assets. The threats to be countered by total defence cut across national borders and the domestic administrative domains of various public authorities. As a result, threat containment demands joint solutions and close coordination among the accountable international and national authorities (The Danish Defence Agreement 2005-2009)	The Estonian definition narrowly focuses on military threats, while elsewhere the Total Defence concept has evolved to encompass the use of all available resources in relation to a full range of threats that can disrupt the functioning of state and society (and thus has become synonymous with Comprehensive Security).